Technology and law

Poullet, Yves

Published in:
Information quality regulation : foundations, perspectives, and applications

Publication date:
2004

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

Technology and Law: From Challenge to Alliance

Yves Poullet*

Table of Contents

This article is a vastly modified version of an article written originally in the French language by the author for the G. Horsmans' Honorary Publication. The English translation has been done by Ariane Deruy, stagiaire at the European Court of Justice.

I. Introduction

1. Information Quality represents an open concept with a lot of different meanings corresponding to the efforts of various actors who sometimes have opposing interests. So as regards consumers, information quality might notably imply correct, updated and not misleading information on products or services offered but also about their providers. The value of information for companies offering web services will depend on the richness of the information they might collect about their potential consumers in order to develop one to one marketing, which is quite opposed to the consumers' privacy requirements. For a citizen facing an administrative procedure, information quality means that the management process of the information delivered by the administration is able to lead to an efficient, transparent and adequate processing of his file. Within the Information Society, information quality might be pursued by different means: managerial, technological and legal requirements. It is quite obvious that these requirements can have cumulative effects: so the legal provision on data security within privacy legislation implies the adoption of both technological and managerial measures in order to protect the confidentiality of the information. In other cases technology might be used consciously or unconsciously against legislative concerns.

In the context of our seminar I have chosen to examine the contradictions and ambiguous relations between law and information or communication technology and law (I.C.T.) as regards Information Quality.

However, there are numerous aphorisms about the relations between law and technology.[1] Is it not a known fact that law always lags behind the technology that dictates its movement? Is it not certain that the Internet's technology revolutionizes law? My ambition is not to give a final answer to these questions but rather to raise some hypotheses: the first ones aim to discover the functions of technology *vis à vis* the law: the role of technology in challenging the legal system is commonly asserted, but technology also has the role of supporting the

On the relations between Law and Technique *see* the remarkable thesis of S. GUTWIRTH, „Waarheidsaanspraken in Recht en wetenschap, Antwerpen, Maku, VUB Press, Thesis, pp. 462 *et seq.* about the intermediary and autonomous function of the law v.a.v. technological developments.

interests promoted by law at the expense of distorting it, as will be demonstrated below (Section II). The second analysis emphasises the relations between law and the state of technology as regards certain restrictions that are undertaken by the latter and even the expectation that the state of technology would be in the law's service (Section III).

Some advice to jurists will conclude the examination of these hypotheses.

II. Technology's Confrontation with the Law

2. The revolutionary aspect of information and communication's technologies in relation to the law has often been proclaimed. The extent of this relation, however, still remains to be defined. On that point, we will merely follow certain methods (*1*).

Technology's function as an ally of law is less often emphasized. Such a role is nonetheless obvious nowadays where everybody requires security on the Internet and understands that it cannot be solely obtained by virtue of the law but would even be better obtained through the use of technology itself: „The answer to the machine is in the machine," declared CHARLES CLARK,[2] as far back as 1996. Probably the demand for security will vary depending on whether it is the investors on the Net that assert its need or whether it is the citizens, customers or the one concerned by the circulation of their personal data on the Net that asserts it. Probably, and this is important for our subject, the security obtained through technology will be of the same nature as that intended in our legislations — and that to the risk of distorting the balance enshrined by law. This will be the subject matter of point (*2*) of this section.

1. Technology's Challenge of Law

3. It appears obvious that technological development offers, to those who wish, the means to undermine legislative order. This sort of challenge of the legal system takes place on three levels: the first one is probably the most obvious: the rules' content is undermined by practices that are made easier by the most recent

CH. CLARK, The answer to the machine, is in the machine, in: The Future of copyright in a Digital Environment, B. Hugenholtz (ed.), Kluwer, 1996, 139-146.

technologies insofar as the respect of such rules is made more difficult. This will be the first point of our reflection. The second form of challenge does not deal with the content of the rules but rather with their author. The standardization of the behaviours that are induced by technological choices is no longer the act of authorities authorised by our constitutions or laws, but by obscure and not very open private authorities whose legitimacy is less than obvious. The third point dwells on the consequences of the global character of technology that induces the loss of national sovereignties, which were traditionally relying on their territories in order to give effectiveness to the protection of rules and values chosen democratically.

a) An Undermined Content!

4. M. FROOMKIN[3] had entitled a recently published article „The Death of Privacy." In that article, the author demonstrated with supporting evidence how the rapid dissemination of technologies both by administrations and enterprises rendered obsolete the rules regarding privacy. Other authors[4] mention the „Privacy Killing Technologies" that enable the tracing of Internet usage, their profiling, „Ubiquitous surveillance,"[5] spying upon information systems,[6] etc.

A. M. FROOMKIN, The Death of Privacy?, 52 Stanford Law Review, 2000, 1461 *et seq.*

See J-M. DINANT, Electronic Threats on personal data and electronic data protection on the Internet, in: Law and Technology Convergence (Sect.5), E-Commerce Law and Practice, ECLIP Network, J. WALDEN & J. HÖRNLE (ed.), Woodhead Publishing, 2002; M. ROTHENBERG, Fair Information Practices and the Architecture of Privacy, 2001 Stan.Tech.L.Rev. 1, n° 62 *et seq.*, mentioning „Privacy Invasive Technologies" (PITS).

For example, the new Internet protocol IPv6 that facilitates the addressing of all the terminals using the Internet (that is, besides the actual I.P addresses, the new generation of telephony or mobile phones using the Internet, the electronic directory, etc.), and this independently of their location. On this new protocol developed by IETF, *see* „Is I.P. v6 finally gaining Ground?" in: Computer, IEEE Computer Society, August 2001, pp. 11-15 and especially Opinion 2/2002 (WP 58) drafted by the Article 29 Data Protection Working Party on the use of unique identifiers in telecommunication terminal equipment: the example of IP v6, May 30, 2002.

6 Since cookies, the information systems' designers improved their so-called Spyware techniques (on that subject, *see* J.M DINANT, footnote 5). Concerning all these systems, *see* the working document (WP 37) of the Article 29-Data Protection Working Party „Privacy on the Internet—An integrated Approach to On-Line Data Protection," November 21, 2000.

Advanced justifications for the development of such technologies rely on the public security,[7] argument and the counter-techno-criminality[8] argument rather than on the willingness to improve the customers' service by a direct maintenance intervention on systems where the software is installed by „one to one marketing."

5. The plagiarism of intellectual „works" on the Internet represents another major concern. The digitalisation of sound, visual or written works, the network and terminals capacities together with compression technologies explain this fact. Firstly Napster then the „peer to peer" software such as Kazaa, Gnutella, Grokster, etc., widely illustrated this reality. Some[9] did even exclaim a few years ago that copyright was dead or, to be more correct, remained pointless at a time where publication of copies of works in unknown places and all over the world made investigations useless.

b) „Authors" without any Constitutional Status

6. In an article published in 1993, J. Reidenberg[10] already underlined the gap between two worlds: the one of the regulation of operations and the one of technical standardization. The first world unquestionably belonged to the traditional competence of national legislators, but the extent of the questions required more and more cooperation within international or local organisations. The second world emerged at that time: the standardization of a global infrastructure such as the Internet required that decisions could only be made

For instance, the authorization given to judicial and police authorities to access Internet traffic and location data (*see* for example in the United States, the Carnivore project or on a worldwide scale the Echelon system).

In particular, the fight against illegal copying of works. On this phenomenon, *see* the figures and the studies mentioned by JAN KAESTNER, Law and Technology Convergence: copyright, in E-commerce Law and Practice in Europe, ECLIP Network, I. WALDEN & J. HÖRNLE, Woodhead Publishing Ltd, Cambridge, 2001.

See especially, T. VINJE, A brave new world of technical Protection: will there still be a room for copyright ?, EIPR, 1996, n° 8, p. 430 *et seq.*

0 J. REIDENBERG. From the same author, *see* the articles published since, Governing Networks and Rule-Making in Cyberspace, 45 Emory Law Journal, 1996, 912 -930; Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 Texas Law Rev., 1998, 553-593.

within bodies known as specialists in technical regulations. These bodies were worked out by pioneers of the Internet with yet unsure competencies.[11]

These bodies, such as IETF,[12] W3C,[13] IANA that became ICANN,[14] have, while at the same time the Internet was spinning its web, acquired, without denying their status of origin, their letters patent of nobility—sometimes with the complicity of governments[15] or of international organisations.[16]

11 On these different bodies of technical standardization as regards information and communication technology, *see* P. TRUDEL (ed.), Droit du cyberespace, Montréal, Thémis, 1997; J. BERLEUR- Y. POULLET, Quelles régulations pour l'Internet, in Gouvernance de la société de l'information, Cahier du CRID, n° 22, Brussels, Bruylant, p. 133 *et seq.*

12 Concerning Internet Engineering Task Force (I.E.T.F.), *see* M.A. FROOMKIN, Habermas @ discourse.net: Toward a critical theory of cyberspace, 116 Harv. Law Rev., 2003, p. 800 *et seq.*; S. BRADNER, IETF Working Group Guidelines and Procedures, available at http://www.ietf.org/rfc.

13 Concerning the W3C's control of the development of HTML and other Web standards, *see* S.L. GARFINKEL, The Web's Unelected Government, MIT Technology Review, 38.46 November 30, 1998 available at http://www.technologyreview.com/articles/garfinkel1198.asp. For the functioning of W3C and its links with IETF, *see* the W3C website http://www.w3.org/Consortium.

14 On ICANN's history, *see* J. WEINBERG, ICANN and the problem of legitimacy, 50 Duke Law Journal, 187 (2000).

15 In this respect, regarding the United States Department of Commerce's supporting ICANN's creation and the will of the American government to put ICANN in control of Internet governance, *see* the articles of A.M. FROOMKIN, Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution, 50 Duke L.J., 2000, p. 17

Who does not understand that beyond a technical standardization, as the attribution of domain names,[17] the Internet addressing, infrastructure's designs, the definition of the technology filtering protocols of contents, etc., the crafting of these technical regulations relates to decisions the content of which would have at another time been taken by authors subject to a constitutional legitimacy.[18] Such an assertion is at the heart of the work that has without any doubt left its mark on legal literature and even on public opinion as regards the relations between law and technology: „Code and other Laws of Cyberspace" by LAWRENCE LESSIG.[19] According to L. LESSIG, the technical architecture, the network's characteristics (protocols, standards of communication that are retained...) create an environment permitting some behaviour and prohibiting others and thus play an essential role in the regulation of cyberspace. Moreover, it is noteworthy to observe that legislators and judges would have to take into account this framework of technological rules which was decided elsewhere than within the traditional law boundaries.[20]

et seq.; Form and Substance in Cyberspace, Northwestern School of Law of Lewis & Clark College, 2002, p. 93 *et seq.*

16 For example the liaisons between WIPO and ICANN. To the contrary, the battle between IETF and ISO (International Standard Organisation) on the choice between the TCP/IP protocol and the OSI model layers must be mentioned. The choice of the private organisation finally prevailed.

17 On this subject, *see* the remarkable article of J. REIDENBERG, Lex Informatica: The formulation of Information Policy Rules through Technology 76 Texas L. Review, 1998, pp. 553-584 and the basic book: L. LESSIG, Code and Other Laws of Cyberspace, New York, Basic Book, 1999.

18 Concerning the debatable legitimacy of the technical standardization bodies, *see* A.M. FROOMKIN, Habermas @ discourse.net: Toward a critical theory of Cyberspace, 116, Harv. Law Review, p. 751 *et seq.* (2003). On the emergence of private „powers" and their regulating function, *see* F.OST & M. VAN DE KERCKOVE, De la pyramide au réseau? Vers un nouveau mode de production du droit, Rev. Interdiscipl. d'études jurid., 2000, 44, p. 66 *et seq.*

19 L. LESSIG, Code and other Laws of Cyberspace, New York, Basic Books, 1999, *available at*: http://www.cyberlaw.stanford.edu/lessig/content/index.html. According to Lessig, the Internet's regulation results from the interaction of four methods of regulation: law, social rules, market and technical architecture.

20 On this interaction between technical regulation and traditional regulation, *see* J. REIDENBERG, Privacy Protection and the Interdependance of Law, Technology and Self-regulation, in: Variations sur le droit de la société de l'information, Cahier du Crid, n° 20,

c) *The Questioning of State Sovereignty*

7. The national state exercised its sovereignty within the boundaries of its territory.[21] Technology puts this „sovereignty" into question in numerous ways:

- the easy dematerialization of essentially immaterial investments that constitute the technological innovation. This fact leads our states either to harmonize their legislations[22] or to launch themselves in a sort of dumping regulation[23] capable of attracting such investments.
- the elimination of boundaries: the very architecture of the infrastructure, its network architecture and elimination of distance as a cost factor of the transmission, leads to the multiplication of conscious or unconscious cross-border flows. It should be pointed out that the majority of Internet root-servers are located in the United States[24] and that messages

p. 130 *et seq.*; Y. POULLET, How to regulate Internet: New Paradigms for Internet Governance, published eod. loco, p. 79 *et seq.*

21 On the intimate links between „State and territoriality" and their questioning by the emergence of immateriality, *see* H. RUIZ FABRI, Immatériel, territorialité et Etat, Arch. phil. droit, T.43, 1999, pp. 187-212: „Le développement des communications immatérielles et la porosité de l'Etat à leurs mouvements posent la question de la maîtrise de l'Etat d'un espace normatif national normalement calqué sur le territoire et exprimé dans le principe de territorialité." *See also*, F. CONSTANTIN, L'informel internationalisé ou la subversion de la territorialité, in: B. BADIE & M-C. SMOUTS (ed.), L'international sans territoire, Cultures et conflits, n°21/22, 1996, pp. 311-345.

22 In a recent article, (Vers la Confiance: Vues de Bruxelles - Quelques considérations sur la spécificité de l'approche réglementaire européenne du cyberespace, Lamy, Droit de l'informatique et des réseaux, 2001, n°141 and 142) the author fully describes this phenomenon at the European level and the harmonised methods that were retained.

23 *See* on this phenomenon, R.QUECK-Y.POULLET, Internet et le droit: Conclusions, Cahier du Crid, n° 19. On the contrary, as regards intellectual property, it will be the country that offers the maximum protection that will attract investments: *see*, D.L. BURK, Virtual Exit in the Global Information Economy, 73 Chicago Kent L.Rev., 1999, n°4, p. 953 and 954: „We may therefore expect that a jurisdiction's 'intellectual property' comparative advantage may assume considerable importance in determining the physical location of information producers." The author (p. 970 *et seq.*), while referring to the „prisoner's dilemma," demonstrates the reasons that can lead the regulators to cooperate or, on the contrary, to prefer competition.

24 10 rooters out of 13 are located in the United States.

transmitted via satellites or by other transmitting media can be subject to interception by foreign powers.[25]

Most probably, international private law rules still enable our jurisdictions to assert the pre-eminence of national law sovereignty,[26] but their decisions will often be confronted by the impossibility of ensuring its application within a network without any borders.[27]

2. Technology's Assistance to Law

8. Through a second evolution, almost opposite to the first one, technology gave law assistance. Firstly, our purpose is to describe this evolution as regards two areas: the one relating to privacy and to intellectual property; some technological developments' objectives are clearly to ensure the protection of interests that are also protected by law. If the expression „Privacy Enhancing Technologies" (PETS)[28] has been promoted in order to designate the technologies that protect our private life, we can henceforth talk about „Intellectual Property Enhancing

25 This is the case of the Echelon satellite information network. About Echelon, *see* J.M. DINANT & Y. POULLET, Le réseau Echelon existe - t'il? available at the CRID's web site: http://www.crid.ac.be and essentially, D.YERNAULT, De la fiction à la réalité: le programme d'espionnage électronique global „Echelon" et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'Homme, Rev. Belge de droit int., 2000, p. 136 and seq.

26 *See* the recently defended thesis of B. DE GROOTE, Onrechtmatige daad en Internet—Een rechtvergelijkende analyse van art. 5, sub. 3 EEX—Verordening en de Amerikaanse bevoegheidsregeling aan de hand van het internet, Thesis, RUG, Jan. 24, 2003 (forthcoming).

27 The Yahoo case fully illustrates this truth. The May 22nd and November 20th rulings of the Paris tribunal (available at http://www.juriscom.net along with an entire file on that case) ordered Yahoo, an American organisation, to filter for French internet users certain revisionists' web sites that are illegal under French law. These rulings have been considered an infringement on the freedom of expression by the ruling U.S. District Court (Yahoo Inc. v. LICRA, July 7, US. District Court California, San Jose Div.) . *See* on that subject, J.REIDENBERG, „Companies will have to comply with the laws where they target business" *available at* http://www.juriscope.net/en/uni/doc/yahoo/reidenberg.htm.

28 About this terminology and a PETS typology *see* among others, H. BURKERT, Privacy Enhancing Technologies: Typology, Critique, Vision, in: Technology and Privacy: New Landscape, AGRE & ROTENBERG (ed.), New York, 1992.

Technologies" (IPETS)[29] and even about „Consumer Protection Enhancing Technologies" (CPETS).[30]

Secondly, it will be demonstrated throughout the same examples, notwithstanding the identity of protected interests, how technologies appreciably modify the paradigms that are the basis of legislations enshrining those same interests.

a) About „Rights Enhancing Technologies"

9. Before moving on to the two topics we have reserved for discussion, PETS and IPETS, we should underline what was probably the first example historically and point out its implications. We will remember that the American legislature had considered that a specific legislative solution was necessary in order to fight against harmful messages, in particular towards minors, and had adopted a legislation known as the „Decency Act." The Supreme Court ruled that the legislative text was infringing the first amendment.[31] Among the numerous arguments, the one that was certainly of most importance was that legal restriction of the freedom of expression is not necessary when less restrictive

29 On these multiple forms of technologies protecting copyright, *see* JAN KAESTNER, Law and Technology Convergence: Copyright, in: ECLIP Network, I. WALDEN AND J. HÖRNLE (ed.), Woodhead Publishing Limited, London.

30 This neologism represents a series of technologies permitting better consumer information (for example, the flickering system enables the consumer to pay attention to certain contract clauses, the pop-up system appears automatically in order to give some additional explanations), better negotiation of contracts concluded electronically (for example, the summing-up of all transactions dealt with on the web site, the automatic error detection system, etc.), a better transaction preservation system (archiving system with a direct access to the concluded operation) even facilities in case of problems linked to the contract execution (hot line, on-line negotiation system in case of complaint, the possibility to access an electronic system of mediation (On Line Dispute Resolution mechanism, etc.)).

31 On the genesis of the Decency Act and the Supreme Court's criticism of it, *see* D. CUSTOS, Liberté d'expression des adultes et protection des mineurs sur le réseau Internet selon la Cour suprême des Etats-Unis, Reno v. ACLU, 26 june 1997, Rev. Dr. Public, 1998, p. 45 *et seq.*; C. LAMOULINE & Y.POULLET, Liberté d'expression et autoroutes de l'information, Rapport pour le Conseil de l'Europe, Nemesis, Bruylant, 1997, in particular pages 69 *et seq.*

technological measures can ensure the protection required.[32] These were the stakes and objective of the development of „Platforms for Internet Content Selection" (PICS)[33] by W3C.

It will enable parents, through a software system linked to a labelling of web sites, to *a priori* define web sites that are acceptable in various regards: „vocabulary, sex, nudity, violence." It is not our intention to recall some of the criticisms that were made but to underline here the advantages of a technical system whose effectiveness is much better than the one relying on costly judicial resources, with uncertain outcome and doubtful enforcement in an international context. It will not surprise anyone that the technological answer has been preferred to the proposed legislative answer.[34]

10. The „Platform for Privacy Preferences,"[35] which was developed by the W3C and considered as the most advanced form of the PETS, is driven by the same principles. It provides, for anyone who wishes, a tool that enables him or her to define his or her preferences as regards privacy and to exclude *a priori* all visits to web sites that do not fulfil such preferences even if it means authorizing a dialogue *a posteriori* with such web sites in order to obtain this or that advantage in exchange for data or in exchange for the authorization to use this or that data.[36]

32 On this debate, *see* L. LESSIG, Code and other Laws of Cyberspace, Basic Books, New York, 1999, p. 177 *et seq.*

33 The reader will find a good description of PICS in R.P. WAGNER, Filters and the First Amendment, 83 Minn. L. Rev., (1998), p. 755 *et seq.*

34 Regarding the evolution of the approaches since the legislative approach of the Decency Act, the pure self-regulating PICS and the Bertelsmann approach, utilized in Europe until the emergence of the so-called co-regulating approach based on the Australian model, *see* M. D'UDEKEM-GEVERS & Y. POULLET, Internet Content regulation: Concerns from a European User Empowerment Perspective about Internet Content Regulations, CL&SR, 2001, p. 371 *et seq.*

35 „I welcome this important new tool for Privacy Protection. It will empower individuals to maintain control over their personal information while using the World Wide Web." This declaration was highlighted in the first publication of the W3C with regard to the P3P which had not yet existed. W3C first Public Working Draft of P3P 1.0 Testimonials (19 May 1998), published on the W3C web site at: http://www.w3.org/Press/1998/P3P.

36 About the P3P and its functioning, *see* L.F. CRANOR, Agents of Choice: Tools That Facilitate Notice and Choice about Web Site Data Practices, *at* http://www.research.att.com/~lorrie/pubs/hk.pdf.

11. In the IPETS[37] field, numerous solutions are pointed out, some of which aim to restrict access; others aim to control or even restrict *a priori* the utilization or some utilizations; others finally aim to find *a posteriori* illegal use. In any case, they guarantee that the right owners' interests, or more broadly the interests of the persons having placed the protected information on the market, are efficiently protected. In that sense, they constitute an answer to the fears of a pirate's cyberspace, underlined above.

In order to continue contributing to the efficiency of such technical measures, the law itself had thought well to add a supplementary layer of protection: developing or utilizing a system circumventing technological measures is itself, WIPO asserts, liable to sanctions, the extent of which is left to the different States.[38] Technology assists law, which itself, in an exchange of civilities, assists technology. But, we shall not think too far ahead on the function of law as regards technology and rather examine technology, throughout the examples of P3P and DRMS, which indeed have protectionist effects that put into question the spirit the paradigms inscribe at the heart of privacy protection legislations, on one hand, and intellectual property right legislation on the other hand.

37 *See*, IMPRIMATUR's works, and especially the publication of A. DE KROON, Protection of Copyright Management Information Inst. For Inf. Law, Amsterdam, December 98 available on Imprimatur's web site at: http://www.imprimatur.ales.co.uk/IMP_FTP/cmi1.pdf which recapitulates a very complete list of protective technologies; *see also*, A. STROWEL & S. DUSOLLIER, La protection légale des systèmes techniques, Atelier sur les questions relatives à la mise en œuvre des traités de l'OMPI de 1996, Geneva, December, 6-7, 1999.

38 Article 11 of the Copyright Treaty adopted by the diplomatic conference of the WIPO in 1996 states: „Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights...." On that subject, *see* S. DUSOLLIER & A.STROWEL, La protection légale des systèmes techniques: analyse de la directive 2001/29 sur le droit d'auteur dans une perspective comparatiste, Propriétés intellectuelles, 2001, pp. 10-27.

b) The „Paradigmatic" Changes Operated by the „Rights Enhancing Technologies"

The P3P[39] Example

12. The P3P is, as was previously the PICS, a technology built around the „User Empowerment"[40] myth. Thanks to an enhanced browser configuration, the Internet surfer can decide which data he will accept to transfer, determine their use, choose to use a pseudonym, etc. If necessary he will resign any protection afforded to him by legal provisions, permitting without restrictions the use of his health data or other sensitive ones. Such an approach relies in essence on a conception of privacy seen as the user's „ownership" of his personal data. This ownership justifies as much the exclusion of the use of my data by others as the „sale" or at least the transfer of the use of data that are henceforth seen as „commodities"—market values. Such an approach, we can sense, is far from that of our „Privacy" legislations. If these legislations recognise consent as being one of the possible roots of legitimacy of personal data processing, they never recognise it as being sufficient[41] on its own in the sense that every processing has to be evaluated, not from the single individual point of view of the person

39 Concerning P3P, *see* J. REAGLE-L. FAITH, The Platform for Privacy Preferences, Comm. Of the ACM, Feb. 99, vol. 42, n° 2, 48-55, the description is available on the W3C web site at: http://www.w3.org/TR/WD-P3P-preferences, and *see* the criticism offered by the Article 29 Data Protection Working Party created by the Data Protection Directive 95/46: Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standards (OPS): http://europa.eu.int/comm/dg15/en/media/dataprot/wpdoes/wp11fr.pdf. *See also*, P.M. SCHWARTZ, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, Wisconsin Law Review, 2000, p. 749 *et seq.*

40 „Central to this concept of user empowerment is the recognition that, on the internet, individuals and parents are best situated to make decisions about what information flows into the home." CENTER FOR DEMOCRACY AND TECHNOLOGY, An analysis of the Bertelsman Foundation Memorandum, available at the center's web site: http://www.cdt.org. Concerning this already popular notion with regard to PICS and the individual's technical control of illegal or prejudicial contents on the Internet, *see* M. D'UDEKEM-GEVERS & Y. POULLET, *supra* note 35.

41 Concerning this subject, *see* A. PIERUCCI, „Le rôle du consentement de la personne concernée dans le marketing électronique," *Ubiquité*, 2001, n° 9; T. LÉONARD, „E-commerce et protection des données à caractère personnel, Quelques considérations sur la licéité des pratiques nouvelles de marketing sur Internet," *available at* http://www.droit.fundp.ac.be/Textes/Leonard1.pdf.

concerned, but in a more collective manner as part of the information's collector's powers—powers that are strengthened by the contribution of the use of information related to others.[42]

This control justifies state intervention particularly as regards both the legislation enshrining the necessity to maintain an informational balance between the person concerned and the one responsible for processing, and the independent control authority's ability to intervene in that regard.[43] It is a question of settling conflict not on ownership, as might be inferred from the technological measures, but on liberties that are likely to be questioned when, either because of lack of intellectual or financial means, the person concerned is not free to choose to ensure his data protection or not or because the transparency of the latter is such that these choices would be influenced or even dictated.

42 *Compare*: „Consent-based approaches to information rights are weak, more fundamentally, because they do not recognize parameter-setting acts of consent or refusal by society as a whole. Problems of market power and cognitive disability could be offset to a degree by coercive legislation. Consent is definitively atomistic and the political process is by definition collective." J.E. COHEN, Information Rights and intellectual Freedom, in: *X. Ethics and the Internet*, Antwerpen, Interscientia, 2001, p. 18. *See* for a similar criticism on „propertisation" of private life by technical effect such as the P3P, the remarkable article of P.M. SCHWARTZ, Beyond Lessig's Code for Internet Privacy, Wisconsin, Law Review, 2000, p. 743 *et seq.* (especially, p. 787). For an overview of the comparison of the American approach based on personal data property as opposed to the European approach based on shareholder control, *see* Y. POULLET, Pour une justification des articles 25 et 26 en matière de flux trans-frontières, The Report presented at the European meeting: The Future of the European Data Protection Directive, Nov. 2002, Liber Amicorum Bart De Schutter, Maklu, VUB Press, Antwerpen, 2003.

43 Article 8 of the Charter of Fundamental Rights of the European Union distinctly enshrined the right to the protection of personal data and the right to have one's private life respected in order to assert the need to control the purposes of data processing and to maintain the existence of an independent control authority; on article 8, *see* Y. POULLET, Le droit et le devoir de l'Union européenne et des Etats membres de veiller au respect de la protection des données dans le commerce mondial, in Le droit et le devoir de l'Union européenne et des Etats membres de veiller à la protection des données personnelles, to be published in a collective work for the XXVth anniversary of the Spanish Constitution, Madrid, Dykinson, 2003, n° 11 *et seq.*

ii. The D.R.M.S. Example

13. SEVERINE DUSOLLIER[44] wrote, „[d]ans l'environnement analogique, l'accès à l'œuvre par le public et sa consultation ne nécessitent aucune autorisation de l'auteur. Lire un livre, voir un film, assister à un spectacle, regarder des œuvres plastiques n'implique généralement dans le chef de l'utilisateur, aucun acte soumis au droit d'auteur, qu'il s'agisse d'un droit de reproduction ou de communication au public."

Some technical devices for work access management enable the control of not only the initial access to the work, but also check the use conditions of every new access; they will set a price according to the use model requested or will require new payment at every new use. These systems rely on the sending of passwords or on the use of encryption techniques.[45] After having described technologies in that way, the author[46] concluded,

> [e]n matière de cryptographie et d'accès sécurisé, la technique n'épouse plus parfaitement les prérogatives de l'auteur. Il ne s'agit plus seulement de renforcer l'effectivité des droits exclusifs, droits de reproduction, de communication ou droit moral, par exemple, par le fait de la technique mais bien d'exercer de manière automatisée la gestion d'un service de distribution de contenus digitaux, qu'ils soient protégés par le droit d'auteur ou non.[47]

Moreover, such technological systems of protection of works undermined the possibility of taking advantage of a series of exceptions to the author's exploitation right which were precisely granted by the legislator in order to promote intellectual creation.

44 S. DUSOLLIER, Incidences et réalités d'un droit de contrôler l'accès aux œuvres en droit européen, in *Le droit d'auteur: un contrôle de l'accès aux œuvres*, Cahier du CRID, n° 18, Bruylant, 2000, p. 26 *et seq.*

45 These different techniques are described in a very detailed manner by J. KAESTNER, *supra* note 29. *See also* D. GERVAIS, Electronic Copyright Management Systems in a Network environment, *available at* http://www. Copyright.com/sruff/ERMSnetwork.htm; and from the same author, The Law and Practice of Digital Encryption, May 1998 *available at* http://www.imprimatur.ales.co.uk/IMP_FTP/encryption.pdf.

46 S. DUSOLLIER, *supra* note 44, p. 40 and 41; T. VINJE, A Brave New World of Technical Protection Systems: Will There Still Be Room for Copyright, *EIPR*, 1996, n° 8, 431.

47 S. DUSOLLIER, *supra* note 44, p. 41; J. COHEN, Information Rights and Intellectual Freedom, in: Ethics and the Internet, ANT. VEDDER (ed.). Antwerpen, Interscientia, 2001, p. 20.

Progressively, thanks to these technological measures,

> [i]t has become conventional to equate ownership of intellectual property with perfect control.... In the context of intellectual property, however, the economic justification for ownership—as—perfect—control is contested....
>
> ...A system of intellectual property rules and rights designed to promote intellectual freedom also must consider the conditions of public access to and use of intellectual goods.... Defining ownership as perfect control forecloses evaluation of these shifts in the distribution of costs and benefits flowing from the intellectual property regime and the resulting effects on intellectual freedom.[48]

III. Law's Confrontation with Technology

14. The position law takes in confronting technology is of a dual nature. It first of all has to welcome the development which is represented by technological innovation in security and surveillance, according to the principle of technologic neutrality, on the one hand, not to discriminate against it but, on the other hand, not to promote it. These two initial aspects will be the subject of our first point. Law can moreover be demanding, and, taking into account the possibilities that are encompassed within the technology, may require that choices be imposed on its development—either in order to guarantee conformity with the law of operations which is enabled by technology, or to improve again the protection of its users. These last attitudes of the Law will be the subject of our second point.

48 J. COHEN, *supra* note 42, p. 27. Same reasoning from A. DIAS-PEREIRA, Copyright Issues of Techno-Digital Property, Intellectual Property in The Digital Age; Challenges for Asia, C. HEATH & A.K. SANDERS (ed.), Kluwer, 2001, p. 66: „The concept of property has a major role in Digitalia and it seems to make sense. However some argued that the new wine could not fit in the 'old bottles'. The new wine would be digital Information property and technologies and the 'old bottles' would be traditional legal concepts, in particular copyright and other forms of intellectual property;" *see* in that respect, P. SAMUELSON's article (The Copyright Grabed, Wired, 1996, quoted by PEREIRA, *supra*, p. 67), that defined the „maximalist agenda" of societies of entitled beneficiaries, aiming to progressively transform intellectual property rights into a plain and simple property right.

1. Law and the Neutral Welcome of Technology

15. The introduction revealed two meanings of the principle of technologic neutrality: the first one is to prevent the law from constituting a barrier to technological development (non-discrimination principle). This attitude characterizes especially recent legislations as regards evidence and signature. These same legislations will enable us to illustrate the second trend: it cannot moreover be a question of subtracting technological developments from the requirements established in the traditional legislations. The „functional equivalent" theory developed with regard to the electronic signature, which has broadened remarkably since, testifies to this trend. In the fight against cybercriminality, this same principal of technologic neutrality had manifested itself in the assertion of the principle that what was punished off-line should also be neither more nor less punishable on-line.

a) From the Non-discrimination Principle to the Principle of Functional Equivalence[49]: The Law of Evidence and of the Electronic Signature

16. The non-discrimination principle is clearly enshrined in two recent Directives: one concerning the electronic signature and the other one concerning certain aspects of electronic commerce.

For instance, article 5.2 of the Directive 1999/93/CE of 13 December 1999 on a Community framework for electronic signatures[50] states: „Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: in electronic form, or not based upon a qualified certificate, or not based upon a

49 On this notion of functional equivalent, *see* in international doctrine, E. CAPRIOLI & R. SOREUIL, Le commerce international électronique: vers l'émergence de règles juridiques transnationales, JDI, 2, 1997, especially, pp. 380-382. Under Belgian legislation, *see* D. GOBERT & E. MONTERO, La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle, *DA/OR*, n° 53, 2000, pp. 17-39.

50 O.J. 19 January 2000, L13/12. On this provision, *see* among numerous authors, M.ANTOINE & D.GOBERT, La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur Internet?, JTDE, 2000, p. 73 and following D. MOUGENOT, Droit des obligations- La preuve, Répertoire Notarial, special ed., Brussels, Larcier, 3ème éd., 2002, n° 121 *et seq.* (especially p. 168).

qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device." Article 9.1 of the Directive 2000/31/CE of 8 June 2000 on certain legal aspects of information society services[51] echo in almost similar terms the same principle: „Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."

17. If the non-discrimination rule reads as a negative version of the principle of technologic neutrality—„the state of technology cannot be excluded solely on the grounds that...," the functional equivalent theory represents the positive version: „the state of technology has a judicial value equal to the one conferred to the traditional state provided that it demonstrates its capacity to realise the same functionalities as the traditional state." This theory expressed for the first time in 1995 by the CRID as regards electronic evidence,[52] has since been largely developed by international[53] and European authorities with regard to signature and writing[54] and was extended in Belgium in an original manner with regard to contractual formality. For instance, article 16 of 17 March 2003 Act on Electronic Commerce[55] asserts that „tout exigence légale ou réglementaire de

51 O. J. 17 July 2000, L 178/1. On this provision, *see* especially P. LECOCQ & C. BIQUET-MATHIEU, Le commerce électronique: conclusion et preuve du contrat, Rapport de droit belge in Actes du Congrès de Brisbane, July 2002, Bruylant.

52 M. ANTOINE, J.F. BRAKELAND & M. ELOY, Le droit de la preuve face aux nouvelles technologies de l'information, Cahier du Crid, n°7, 1995, Story-Scientia, Brussels.

53 *See* on the subject the guide to enactment of the UNCITRAL Model Law on Electronic Commerce, 1996, especially n°16 that precisely lists the writing's functionalities.

54 *See* especially among numerous authors, M. DEMOULIN & E.MONTERO, La conclusion des contrats par voie électronique, in: Le processus de formation du contrat. Contributions comparatives et interdisciplinaires à l'harmonisation du droit européen, M.FONTAINE (ed.), Brussels-Paris, Bruylant-LGDJ., 2002, Vol.57, p. 550 *et seq.* Authors give another example of functional definition, the one of „durable medium," concerning some traditional medium as some numerical medium, this notion is used in the Directive 97/7 called „distance contracts" and is finally defined in the Directive of 23 September 2002 concerning the distance marketing of consumer financial services.

55 Law of 11 March 2003 on certain judicial aspects of the information society services, M.B., 17 March 2003, p. 12693.

forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées." MONTERO[56] justified this provision as follows:

> En présence d'un tel obstacle (à savoir celui né de l'impossibilité de réaliser les exigences formelles imposées par les dispositions réglementaires consacrant le formalisme contractuel), l'article 16 § 1er nous invite à adopter une approche dite „fonctionnelle". Il s'agit de rechercher quelles sont les qualités fonctionnelles de la formalité considérée, puis de vérifier si le procédé utilisé pour conclure le contrat par voie électronique permet de préserver ces qualités. Dans l'affirmative, l'exigence de forme est réputée rencontrée par le procédé en question et le contrat conclu par voie électronique ne peut être remis en cause à cet égard.

Therefore, the law recognises as its duty the welcoming of technologic developments that substitute traditional conclusion processes of execution or conservation of contracts when these developments guarantee the respect of functional requirements, which originally justified the recognition of the traditional processes.

b) *From the Principle of Technological Neutrality or the Necessity of an Equivalent Judicial Framework*

18. The principle of technological neutrality has at least two meanings: the first one advises cautiousness to the legislator—that is, when he legislates to refrain from any reference to a particular technology that might prohibit technological progress[57] later on.... Therefore, the initial laws concerning electronic

56 M. DEMOULIN & E. MONTERO, Le formalisme contractuel à l'heure du commerce électronique, in : Commerce électronique: de la théorie à la pratique, Cahier du Crid, n°23, Brussels, Bruylant, 2003, p. 161. *See also*, D.GOBERT & E.MONTERO, Le traitement des obstacles formels aux contrats en ligne, in: E.MONTERO (ed.), Le commerce électronique enfin sur les rails? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique, Cahier du CRID, n°19, Brussels, Bruylant, 2001, p. 199.

57 Concerning the application of the principle in the context of the Directive 2002/58/CE which concerns the processing of personal data and the protection of privacy in the electronic communications sector, *see* the reflections of J. DHONT & K. ROSIER, Directive vie privée et communications électroniques: premiers commentaires, Ubiquité, 2003, n°15, p. 45: „Par rapport à la directive 97/66/CE, la nouvelle directive est novatrice en ce sens qu'elle prévoit des règles indépendantes de al technologie mise en œuvre. Ce cadre neutre devrait être garant de la certitude juridique et rendre superflue toute modification de la législation en fonction des avancées technologiques...L'effet paradoxal qui en découle

signatures, the one from Utah, an American state, or from Germany revealed themselves as being rapidly out-of-date in the sense that the terminology employed prohibited the recognition of some signature processes which were more reliable than the one enshrined by law.[58] The second meaning is more important here: it is to avoid providing a different destiny to the operations taken via electronic processes as compared with the one dedicated to the operations taken via traditional processes.

19. The law of 28 March 2000 concerning cybercriminality[59] is based on the simple and sound principle that any operation suppressed off line should be neither more nor less suppressed when it is realised on line.[60] Probably, according to the principle of strict interpretation of criminal texts, new infringements should be created, but the conditions given for the recognition of such infringements should be copied as best as possible on those existing in the traditional infringement framework. The perpetration of an infringement through the use of technology or connected with information systems can, on the one hand, indeed go unpunished but, on the other hand also does not deserve a regime aiming to mislead natural persons. The use of processes in order to deceive a machine deserves neither more nor less legal sanction. Probably this principle of technologic neutrality has not always been respected when we closely analyse the texts, and some deplore a hardening of suppression of this new form of criminality,[61] but this is not the subject of our present discussion.

est que pour pallier les incertitudes liées à l'évolution technologique future, on recourt à des termes imprécis, qui sont eux-mêmes source d'incertitude juridique."

58 The reader may on that point refer to the demonstration of GOBERT & MONTERO, *supra* note 56, pp. 73-78 and especially n° 4.

59 Law of 28 November concerning cybercriminality, M.B., 3 février 2001, p. 2909 *et seq.*

60 *See* in that respect, the following passage of the Preamble: „Si le droit pénal nécessite certaines modifications pour tenir compte des spécificités de la criminalité informatique et ce, afin de respecter le principe *'Nullum crimen sine lege'*, il ne faudrait pas que ces adaptations du droit pénal aux progrès technologiques aboutissent à sanctionner un type de comportement alors que si ce même comportement avait été commis sans l'aide de l'informatique, il n'aurait peut-être pas donné lieu à une répression pénale."

61 Concerning the definition of „computer forgery" compared to „ forgery," *see* O. LEROUX, note under Civ. Liège 18 nov.2002, Ubiquité, 2003, p. 96 *et seq.*, concerning the „hacking" or unauthorised access of information systems, *see* the reflections of S. DUSOLLIER & F. DE VILLENFAGNE, La Belgique sort enfin ses armes contre la cybercriminalité, Auteurs et Medias, 2001, p. 60 *et seq.*

2. The Law's Requirement that Technology Guarantee that Operations Conform to the Law Even Where it Improves the Situation of Persons Protected by Law

a) The Principle of Proportionality or of Reciprocity as Regards Technological Advantage

20. This principle could be expressed as follows: the legislator, at any possible time, in order to enable the restoration of the traditional balance of the participating parties, imposes additional obligations on the one who is using technologies with the view to develop his professional activities.[62] The justification of the principle is simple: if technology increases the capacities for information gathering and processing and its dissemination to others, where technology is used to conclude transactions or administrative operations, it is necessary that this same technology be configured and used in a way that the person concerned, the citizen, the consumer, can benefit to a „proportional" extent from the advantages of technology.

21. The Belgian legislation's application of this principle only concerns, at the present state, the commercial services of the information society. Foreign countries, however, give us examples of other possible explanations as regards, in particular, electronic administration or privacy.

Proportionality and Information Society Services

22. Concerning the commercial services of the information society, the Directive 2000/31 on certain legal aspects of information society services, cited above, increases in this respect the obligations for „services providers of the information society" to use the technologies' resources and does so for different purposes: to notify the Internet surfer of the advertising character of the service provider's messages[63] and to inform him in an easily accessible way of the codes

62 We have developed this principle in two articles: concerning the regulation of electronic contract, Y. POULLET, Contrats électroniques et théorie générale des contrats, Liber Amicorum L. Simont, Bruylant, 2002, p. 469 *et seq.*; en matière de protection des données, Internet et vie privée: entre risques et espoir, J.T., 2000, Le droit des nouvelles technologies, n° spécial, p. 162, n°26.

63 That will enable the Internet user to filter them by adequate technological means.

of conduct to which he has agreed, of the different stages followed for the contract conclusion, and of the available techniques for the identification and the correction of possible mistakes. Such information must be easily accessible at any time and downloadable.[64]

Some authors[65] underline, with regard to the same principle, that the obligation to describe the good or service offer is to be understood more strictly regarding transactions concluded on the Internet,[66] and that the enforceability of general conditions implies, according to the criteria of „reasonable notice," that the use of techniques not only be hyperlinked, but if need be, be displayed by pop-ups featuring blinking messages, etc.[67]

23. Some recent provisions rely on the proportionality requirement to justify the imposition of obligations on anyone who uses technologies to make available to the Internet user some electronic means to assert his interests or his rights.

We can quote, for instance, in the Directive mentioned above, the possibility to prevent spamming via electronic means,[68] the obligation of suppliers to make

64 ... by explicit acronyms, hyperlink or pop up.

65 *See* in particular, S. CAVANILHAS-MUGICA, Dix thèses sur la protection du « consommateur électronique » d'après la directive sur la vente et les garanties de consommation, Ubiquité, n°7, 2001, p. 99 *et seq.*

66 „La façon de rédiger un contrat électronique ne doit pas être perçue comme étant identique à celle d'un contrat papier et le juriste ou l'avocat doivent adapter la règle au medium. En particulier, les critères de lisibilité, de compréhension voire de raisonnabilité risquent de ne pas être perçus de la même façon selon qu'on les analyse sur un document écrit ou sur un document électronique." V. GAUTRAIS, Les contrats en ligne dans la théorie générale du contrat: le contexte nord-américain, in Le commerce électronique – Le temps des certitudes, Cahier du Crid, n°17, Brussels, Bruylant, 2000, p. 113.

67 Regarding these different techniques and the obligation to use them in order to comply with the „reasonable notice" requirement, *see* M. CHISSICK & A. KELMAN, *Electronic Commerce Law and Practice*, Sweet and Maxwell, 1999, p. 85 *et seq.*

68 *See* article 13.2 of Directive 2002/58/CE concerning the processing of personal data and the protection of privacy in the electronic communications sector which provides for the exercise of the right to object to marketing messages when they are not requested. It is worth noting the recital that specifies that it would be useful but indeed not required that in such cases, the communication service user can identify the sender of the message as well as the subject line of the electronic mail and that he can delete it without having to download it. *See* also, article 14 paragraph 2 of the Belgium Act implementing this Directive which explicitly provides the obligation to make available „un moyen approprié d'exercer efficacement ce droit par voie électronique."

available to Internet users the means for the correction of mistakes[69] and, more precisely, as regards electronic means of payment and signature, electronic notification tools of the loss or theft[70] of such means.

ii. Other Applications

24. The American „Electronic Freedom of Information Act"[71] contains an interesting provision regarding the principle we have evoked here. The Act affirmatively imposes the duty on the Administration to make available to interested citizens via an electronic media any document to which access has been required at least three times according to the law on access to administrative documents.

Recently another American legislation,[72] the „Federal Data Quality Act," was adopted which provides that a citizen's access to his administrative record must be operated electronically. Also a Swedish commission[73] recommended the adoption of legislation that guarantees a citizen the right to electronically follow

69 *See* article 10 of the Directive on certain judicial aspects of the information society services and article 8 paragraph 1 3e of the Belgium Act of 11 March 2003 implementing the Directive on e-commerce.

70 In this respect, *see* article 6 of the law of 17 July 2002 (M.B. 17.8.2002, p. 35337) that provides (article 6) among the issuer's obligations of a means of payment, the obligation to make available to the holder, all means to permit the carrying out of notification of the robbery or loss of its payment instrument.

71 Concerning the „Electronic Freedom of Information Act" of 1996, *see* C. DE TERWANGNE, Droit à l'information et droit à la transparence: vers une société de la connaissance, Doctoral thesis to be published, in Cahier du CRID, Brussels, Bruylant, 2003.

72 This 99 Act enables the Office of Management and Budget to issue guidelines in order to maximise integrity, accessibility, efficiency, transmission, and utility of collected or used data by the administration and binds the administration to internal and external reviews. Concerning this law and the guidelines, *see* the contributions by U. GASSER and H. BURKERT, in this volume.

73 Concerning the recommendations of the Swedish ICT Commission, *see* in the same book, P. SEIPEL, Information System Quality as a Public Concern. H. BURKERT, L'information du secteur public: le secret, la transparence et le commerce, *Rev. fr. adm. Publique*, oct-déc. 1994, p. 588, following the analysis of the Quebec Act on the right of access, talks in this respect of the right of the citizen to „un temps d'ordinateur," which means that the administration files must be programmed in a way that the citizens can electronically exercise their access rights.

the progress of his record from its origin up to and including its archiving. Thanks to technology, a more transparent and more accessible administration for citizens must respond to a more efficient administrative system.

As regards data protection, we can even envisage that certain rights of affected persons—such as the right to information,[74] the right of access and rectification[75]—will tomorrow be realised by electronic means.

b) *The Principle of Promotion of Technologic Solutions that Conform to or Improve the Situation of Persons Protected by Law*

25. In that respect, the law's intervention operates in various ways: firstly, it includes the reservation of the right to intervene in case of technological developments which entail major risks; for some legally protected interests, the obligation to support the risks of weaknesses of technologies for those who use them must be asserted, and independently of any idea of misconduct; furthermore, by imposing an obligation of so-called security, the law obliges those who benefit from technologies in their operations to make sure that they are reliable; finally, technological solutions will be promoted, especially the rules of disputes in order to facilitate users' actions.

We will briefly cover these various methods.

26. The first method is illustrated by a provision of the Directive of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Article 14 provides that when terminal equipment is not compatible with rules of data protection, the Commission can

74 Therefore, the possibility to have direct access, with a simple click, to the „Privacy Statement" of an enterprise and to various information concerning the identity of the responsible entity—even to the declaration made by the responsible entity to the controlling authority or to a specific label given by the labelling authority; as regards the latter point *see* the reflections of J. REIDENBERG, Adapting Labels and Filters for Data Protection, Cybernews, 1997, III, 6 available on the web site of Lex electronica: http://www.droit.montreal.ca/pub/cybernews/htm.

75 *See* in this respect, the recent amendment of the law governing the national register that provides the citizen with an electronic access right to the data concerning him which is in the national register or on his electronic identity card.

take initiatives with regard to its standardisation.[76] In other words, the technical standardisation of terminal equipment constitutes a measure—indeed a subsidiary one—to ensure the protection of personal data against the risks of certain abusive treatment—such risks being created by technological choices.

27. The second method is illustrated by numerous provisions. For instance, according to article 2B of the American Uniform Commercial Code,[77] the risk of programming errors are at the expense of the one who uses an electronic agent in order to conclude a contract, without it being necessary to prove any misconduct of the latter.

The shift of responsibilities based on misconduct to an almost automatic responsibility based on risks created by the use of technologies is obvious in other provisions. The solution is classic as regards electronic payment[78] or electronic signature.[79] The legislature has enshrined classic doctrinal and case-law assertions which held the payment card holder responsible for the consequences of his actions in the case of loss or theft of the card or of the secret confidentiality number, as long as he has not notified the issuing body of the

76 On this provision and its interpretation, *see* M.V. ASINARI & S. LOUVEAUX, Proposal for a directive of the European Parliament and of the Council of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000)385 ECLIP, 2001.

77 R. NIMMER (Electronic Contracting: Legal Issues, 14 Journal of Computer and Information Law, (1996), p. 211 *et seq.*) justifies the solution by the „attribution" theory, which states that the one who creates a false appearance has to bear the risks linked to the consequences of the creation of that false appearance. Concerning article 2B of the UCC and the formation of contracts by electronic agent, *see* our reflections in: la conclusion d'un contrat par un agent électronique, in Commerce électronique - Le temps des certitudes, op.cit , p. 120 *et seq.*

78 In this respect *see*, the hypothesis expressed by X. THUNIS (Responsabilité du banquier et automatisation des paiements, Travaux de la faculté de droit de Namur, n°17, P.U.N., p. 251): „Notre hypothèse est qu'émerge la qualification de 'prestataire de services automatisés' dont la responsabilité se fonde sur une théorie du risque qui ne se réfère plus aux articles 1239 et 1937 du Code civil." Concerning the confirmation of this hypothesis in the recent law of 17 July 2002 (M.B. 17 août 2002, p. 35337), especially with regard to its article 8, *see* the article of A. SALAÜN, Une nouvelle pierre à l'édifice de protection des consommateurs: la loi sur les transferts électroniques de fonds, J.T. 2003, p. 210.

79 *See* on that point the analysis of the provisions regarding responsibility in the European Directive concerning electronic signature and in the model law of the UNCITRAL in Y. POULLET & J.F. LEROUGE, La responsabilité des acteurs de l'Internet, Rapports de droit belge au Congrès de droit comparé de Brisbane, July 2002, Brussels, Bruylant.

loss. The obligation to bear the risks linked to system information use is also present in the Directive on certain legal aspects of the information society when it is asserted that the order and acknowledgement of messages concerning an order procedure are deemed to be received once they arrive at the mail service server, even if the recipient is not yet aware of it. Indeed, from this moment, they have entered the sphere of the risks that are to be insured by the recipient.

28. Article 16 of the Directive 95/46/CE on data protection, the third method, attributes to the person responsible for personal data processing an obligation of security, the extent of which is determined by the risks of impairing confidentiality linked to the system characteristics and to the nature of the data processes as well as to the state of the art as regards technological security as understood in broad terms.[80] It means that the law imposes upon the person who processes personal data the choice of technological solutions that are capable of minimising or even eliminating risks of privacy infringement.[81]

29. The last type of legislative intervention refers to a series of measures which aim to promote the use of technological tools that directly or indirectly ensure the compatibility with the law of operations concluded via electronic systems. On this point, it is difficult to be exhaustive, but we will retain the intention to define and to recommend without necessarily imposing the norms, sometimes technical, sometimes behavioural[82] that will have—it goes without saying—an

80 As regards this security obligation deduced from „Privacy" legislations, *see* D. DE BODT, „De aangestelde van de gegevenscherming inzake de verwerking van persoonsgegevens," *Computer*, 1999, pp. 279-288.

81 The same reflection can be drawn as regards article 8 of the recent law concerning the instruments of electronic funds transfer, which exclude the responsibilities rules of the card holder if the instrument has been used without any physical presentation nor electronic identification of the instrument itself. As it has been noted by A. SALAÜN (*supra* note 78, p. 210), „On trouve ici la principale motivation de la dérogation: éviter que les instruments de transfert électronique de fonds ne puissent être utilisés à distance sans aucune sécurité."

82 In this regard *see* the works of the mcm Institute of the University of St Gallen (http://www.mcm.unisg.ch) which, during its 4th Conference „On Information Quality and Knowledge" dedicated an important part of its works to the subject of „Qualität im Internet." Concerning this tendency towards the standardisation of behaviours, *see* U. GASSER, Variationen über „Informationsqualität," Festschrift für J. N. Druey, Schulthess, Zürich, 2002, p. 750 *et seq.* As regards data protection, *see* the works of the European Committee of standardisation described on the web site: http://www.cenorm.be/isss/Projects/DataProtection.htm, and as regards the conformity of web sites to legal

influence on the design, including the electronic commercial techniques of web sites. The European Commission's recommendations and the recent green paper on alternative methods of the settlement of disputes and the use of electronic systems,[83] aim as well, in that respect, to facilitate actions of Internet users when they encounter difficulties regarding commercial electronic operations. Two Directives, one entitled „electronic commerce" and one on „distance marketing of consumer financial services," echoed this objective in requiring the establishment of „adequate and effective" mechanisms of complaints and actions.[84]

IV. Conclusions

30. The considerations suggested above naturally bring the author to assert some recommendations aimed at jurists facing the technological challenge. The first recommendation invites him to dare to fathom the mysteries of technology, not to get bogged down, but to seize the huge possibilities of its development. The state of technology does not force itself upon the jurist but on the contrary it is a flexible tool, subject to development options and thus subject to choices. Probably some of the choices made will prove irreversible. It is the duty of us as lawyers to penetrate the restricted circles of technical standardisation bodies and to discuss the concrete implication of our legislative requirements.

provisions of a various nature, *see* the Suisse standardization association's works regarding „Online-services" (SNV Workshop Agreement SNR 1) available on the web site: http://www.snv.ch/.

83 In this respect note the recommendations of 30 March 1998 (98/257/CE) on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes (J.O. 17 April 1998) and of 4 April 2001 (2001/310/CE) on the principles applicable to the out-of-court bodies involved in the consensual resolution of consumer disputes. *See* the Resolutions dated from March 30th 1999 of the Commission with regard to principles applicable to the bodies responsible for out-of-court settlement of consumer disputes and of 13 April 2000 of the Council on the creation of a European network for out-of-court settlement of consumer disputes. The green paper of the Commission on alternative dispute resolution in civil and commercial law was published 19 April 2002 and was followed by the European Parliament resolution of 12 March 2003.

84 *See* article 17 of the Directive already quoted on certain legal aspects of information society services and article 23 of the Directive of 23 September 2002, quoted above, concerning the distance marketing of consumer financial services.

These requirements, and this is the second recommendation, probably deserve to be clarified and, this can only be done by the confrontation of jurists with those who work for technological development. It cannot be about the opposition of *a priori* values of law on the one hand and such development on the other. Therefore, we cannot assert, *a priori* that technical measures constitute the end of traditional copyright and of the values carried by the law. It is important to understand the mechanisms susceptible of being established, and to ask oneself about their impact on the significance of subtle balances set down by legislation and the legitimate or illegitimate impact of this mechanism on this balance: e.g., must we keep with the same extension the „fair use" exceptions when today easy, immediate and inexpensive copies are permitted while yesterday these facilities could not be conceived?

Such a task of taking a good hard look at oneself, as technology invites the law to do, requires in return, from technology, a period of waiting. The third recommendation is that we must not be hurried in formulating regulation—neither as regards law destroying the technological developments' possibilities, nor as regards technology making law an unconscious or unconditional ally. Neither can it be a question of not regulating when evaluation demonstrates the inconsistency of development or of certain developments with values that are estimated as being essential in societies which must remain in control of the technological tool.

A fourth recommendation consists of conceiving in a positive way the development of technologies and to find therein the possibility of the most efficient realisation of certain traditional rights, or even the assertion of new rights capable of correcting, to the benefit of certain rights, new imbalances that are introduced by the technological medium.

Finally, the last recommendation: the jurist cannot undertake this work only at the national state level. The global market dimension which technology imposes involves new localities in our dialogue or even compels the search for regulatory consensus. Internet law cannot represent the lowest common denominator but it must enable our various societies to put forward their own values within legitimate international enclosures.