

B2. Ethics and modes of governance of the Internet

*Jacques BERLEUR (IFIP-SIG9.2.2 Chair),
Marie d'UDEKEM-GEVERS and Laetitia ROLIN
Facultés Universitaires Notre-Dame de la Paix, Namur, Belgique
Email: jberleur@info.fundp.ac.be; mgevers@info.fundp.ac.be;
laetitia.rolin@fundp.ac.be*

Introduction³⁵

It is now well recognized that the global network environment, and in particular, the Internet, defies traditional regulatory theories and governance practices. The main reasons are linked to the disintegration of the concepts of territory and sectors. It has therefore been suggested to approach the regulation of the Internet from different points of view, technical, self-regulating and legal, for instance.³⁶

This paper is a first exploration of those challenging issues, but does not pretend to be more than an attempt to assess what is really happening in the different domains of technical mechanisms, self-regulation and the law. We are not looking at what could be done, but at what is done through those different instruments, trying to enlighten which are the ethical issues which are covered by those instruments and which are not. It is a kind of a first inventory.

In this short paper, we tried to summarize the approach we presented during a recent “rolling workshop and round-table” during the fifth IFIP-TC9 Human Choice and Computers international conference held in Geneva, last August.³⁷ This work is the fruit of an on-going working programme within the Special Interest group (SIG9.2.2) “IFIP Framework for Ethics” of the International Federation for Information Processing. We shall analyze the ethical issues, as they appear first when considering the technical means of labeling and filtering, second in a sample of self-regulation systems, and finally in two specific legal questions.

³⁵ This paper is a summary of three papers which were presented during the "rolling workshop" of the IFIP-TC9 HCC-5 conference (Geneva, August 1998). It has been presented, as a result of the IFIP-TC9 HCC-5 Conference at the UNESCO InfoEthics'98. It is reprinted here with the kind authorization of UNESCO. (See http://www.unesco.org/webworld/infoethics_2/index.htm)

The two first authors belong to the Cellule interfacultaire de Technology Assessment (CITA), the third to the Centre de Recherche Informatique et Droit (CRID), which are both sponsored by the Belgian Federal Office for Scientific, Technical and Cultural Affairs, in the Framework of its Programme “Interuniversity Poles of Attraction”, Phase 4, Convention n° 31.

³⁶ Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 *Emory Law Journal* 911, 1996, reprinted in *Borders in Cyberspace*, Brian Kahin and Charles Nesson, eds., MIT Press, 1997.

³⁷ Ethics and the Governance of the Internet, Rolling Workshop and Round-Table at the 5th Human Choice and Computers IFIP-TC9 International Conference, *Computers and Networks in the Age of Globalization*, Proceedings, S. Munari, G. Krarup and Leif Bloch Rasmussen, Eds, Geneva 25-28 August 1998, Printed by the University of Lausanne, pp. 307-387.

Ethical Issues and Questions with Filtering Software

Introduction

Filtering/control software is a technical means, located on a PC or a server or at the level of an Internet service provider, to restrict the distribution of certain kinds of material over the Internet.³⁸ In many cases, its goal is the protection of children against sex, violence, hate speech, etc. (see Table 1).

Labeling categories	Frequency in the sample
sex	7/10
violence	7/10
age	5/10
intolerance/hate speech	5/10
gambling	4/10
drugs	3/10
language	3/10
nudity	3/10
alcohol/tobacco	2/10
profanity	2/10
education content	2/10
gross depictions	1/10
satanic/cult	1/10
militant/extremist	1/10
quality	1/10
etc.	

Table 1 : Labeling categories and their frequency in a sample of 10 ratings³⁹

This kind of software is promoted or supported by industry, Free Speech activists and some governments. Currently a lot of the available control software packages filter at the level of the entry point to an address on the basis only of their proprietary (and secret) list of URLs.⁴⁰

But this could evolve thanks to PICS (Platform for Internet Content Selection). PICS is a set of technical standards which have been developed since summer 1995 by the MIT's World Wide Web Consortium. "The first and most important distinction that PICS introduced is a *separation between labeling and filtering*. A label describes the content of something."⁴¹ A

³⁸ 'Control' and 'filtering' are considered here as synonymous.

³⁹ Cyber Patrol (4.0) (CyberNOTlist), evaluWEB, Net Shepherd's Rating, SurfWatch (for kids), Adequate.com, IT-RA, RSACi, Safe For Kids, SafeSurf's Internet Rating Standard, Vancouver Webpages Rating Service (see M. d'Udekem-Gevers, What can be regulated on the Internet by control/filtering software ?, in: *Computers and Networks in the Age of Globalization*, doc.cit., pp. 315-334).

⁴⁰ An URL (Uniform resource Locator) identifies the location of a document.

⁴¹ « PICS labels can be attached or detached » (and stored on a separate server called a 'label bureau'), Paul Resnick, 1997 Filtering Information on the Internet, in: *Scientific American* 03-97.

filter makes the content inaccessible to some audience.”⁴² In other words, thanks to PICS, “Consumers choose their selection software and their label sources (called rating service) independently.”⁴³ “More generally, there are six roles that could be filled by different entities”, as explained in table 2.⁴⁴

1. ‘Set labeling vocabulary and criteria for assigning labels’
2. ‘Assign labels’ (= rate or classify)
3. ‘Distribute labels’
4. ‘Write filtering software’
5. ‘Set filtering criteria’ (= customize)
6. ‘Install/run filtering software’

Table 2: The 6 roles implied by filtering software (according to Resnick 1998)⁴⁵

Moreover, PICS standards facilitate “*self rating* (enable content providers to voluntarily label the content they create and distribute) and *third party rating* (enable multiple, independent labeling services to associate additional labels with content created and distributed by others. Services may devise their own labeling systems, and the same content may receive different labels from different services.”⁴⁶

PICS would become more and more important. Control software such as Cyber Patrol does not hesitate to become currently PICS compliant.⁴⁷ PICS approach, which separates clearly the different roles involved in filtering, helps to analyze issues and allows solutions which are interesting from an ethical point of view.

Ethical issues with filtering software will be discussed here from the breakdown of table 2. Let us first remark that to ‘set labeling vocabulary and criteria for assigning labels’ is not value-neutral and that to ‘assign labels’ and to ‘set filtering criteria’ imply moral judgements. Any ethical approach has thus to focus on these three roles.

Outside PICS

Outside PICS, it happens as a rule that several roles (particularly to ‘set criteria for assigning labels’ or for classifying, to ‘assign labels’, to ‘distribute labels’ and to ‘write filtering software’) are filled in the framework of one firm or even by one sole commercial entity.⁴⁸

⁴² Paul Resnick last revised 26-01-1998, PICS, Censorship & Intellectual Freedom FAQ, <http://www.w3.org/PICS/PICS-FAQ-980126.html>

⁴³ Resnick Paul and Miller James, 1996, PICS: Internet Access Controls without Censorship, in: *Communications of the ACM*, 39 (10), October 1996, p. 88.

⁴⁴ P. Resnick last revised 26 01 1998, PICS, Censorship & Intellectual Freedom FAQ.

⁴⁵ See <http://www.w3.org/PICS/PICS-FAQ-980126.html>

⁴⁶ See <http://www.w3.org/PICS/principles.html>

⁴⁷ According to several comparative reviews, Cyber Patrol is the best among the tested packages. (see Munro C., 1997, Internet Filtering Utilities, in: *PC Magazine*, April 8 1997, pp. 235-240.; Parental Control Software at a Glance, October 97 issue of *FamilyPC*

<http://www.zdnet.com/familypc/9709/noway/table.html> ; Meeks Ch., 8 programs to porn-proof the Net, 4/3/96; updated 5/28/97 <http://www.cnet.com/Content/Reviews/Compare/Safesurf>)

⁴⁸ The role of ‘assigning labels’ is similar to the one of making a list of URLs to block.

Ethical issues are obvious with this kind of software: *users are linked to the subjective value judgements of this firm* ! Even to 'set filtering criteria' can be reduced by the firm to a nearly virtual role: the only choice available can be, for example, between 'filtered access' or 'not filtered access'.

Within PICS

Within PICS, as explained above, the six roles can be filled by different entities. This can obviously improve the situation from an ethical point of view but cannot delete any issue.

We suggest here a set of questions to be raised and which, of course, remain valid outside PICS.

Set Labeling Vocabulary and Criteria for Assigning Labels

To 'set labeling vocabulary and criteria for assigning labels' is a crucial role. First it influences automatically other steps of the filtering process ('assigning labels' and 'setting filtering criteria'). But moreover, as pointed out by CPSR (1997), "in general, the *use of a filtering product involves an implicit acceptance of the criteria used to generate the ratings involved.*"⁴⁹

- Who is in charge of this role ? Is the identity of the person or the body responsible for this role clearly given in the documentation about the filtering software ? Would it be justified that a government fills this role ?
- Are the rating vocabulary and criteria clearly defined so as to allow the user (parents, ...) to judge if they are consistent with his/her own values ? Are they rich enough to allow a real choice at the level of the rating and at the level of the customization ?

Assign Labels

- Who is in charge of the very sensitive role of assigning labels ? Is the identity of the person or the body responsible for this role clearly given in the documentation about the filtering software ?
- Which of the two approaches (self-rating and third party rating) is the best ?
- When a third party rating service is involved, the next questions are to be raised : Who is effectively represented by this third party ? Is this party representative, for example, of a values-oriented organization or of a given population or culture? How are the ratings attributed?
- With self rating, the questions are : How to oblige or, at least, to incite people to self rate ? And on the basis of which principle ? How to solve the problem of mislabeled pages, and particularly of deliberately mislabeled pages ? As suggested by Cranor & Resnick, "The Internet community will need to co-operate in the creation of either vouching services, which vouch for authors who are honest in their self-labeling, or blacklisting services which keep track of authors whose labels are not reliable."⁵⁰

⁴⁹ CPSR 1997, Filtering FAQ, Version 1.1, 12/25/97, written by Hochheiser H., <http://quark.cprs.org/~harryh/faq.html>

⁵⁰ Cranor Lorrie F. & Resnick Paul, Technology Inventory, 12 March 1998, <http://www.research.att.com/~lorrie/pubs/tech4kids/t4k.html>

- If people assign labels and if labeling is not compulsory all over the world, it is obvious that *many sites will stay unlabeled*. The question is then : What to do with unlabeled sites ? If the software allow unrated sites, then the global control will not be efficient but if it does not, then innocuous and very interesting sites will be not accessible (see the discussion of Weinberg on this subject).⁵¹ And thus in this case, “blocking software could end up blocking access to a significant amount of the individual, idiosyncratic speech that makes the Internet a unique medium of mass communication. Filtering software, touted as a speech protective technology, may instead contribute to the flattening of speech on the Internet.”⁵²
- Can the person or body in charge of the rating use rating criteria in accordance with his/her own value judgements ?
- Are the ratings numerous and various enough to cope with the diversity of cultures and of opinions at the level of the customization ?

Set Filtering Criteria

- Which kind of customization ? In fact there is a dilemma : the more choices you give to the final users the more difficult it is to set ! A solution in the future could be, as suggested by Cranor & Resnick, “to allow users to download preconfigured setting from organizations they trust. Child advocacy organizations as well as various religious, political, and educational organizations might recommend configurations to parents. Parents could download these settings with a simple click of the mouse and have them installed into their child’s software.”⁵³
- Who is in charge of this role? Initially this role was dedicated to parents to control their children. But filtering software are used also by libraries (in the USA), for instance to control adults, by schools and by firms. Is it ethically justified to give such a power of control to this kind of entity ? “A government could try to impose filtering criteria in several ways, including government-operated proxy servers (a national intranet), mandatory filtering by service providers or public institutions, ...”⁵⁴ Would it be ethically justified ?
- Can the person or body in charge of the customization find both criteria and a rating in accordance with his/her own value judgements ?

Governance and Self-regulation

Pierre Van Ommeslaghe defines self-regulation as “a legal technique according to which the legal rules or the rules of conduct are created by the persons to whom they are intended to be applied, - either those persons do it by themselves or they are represented to do it”, but he does explicitly exclude some ‘codes of conduct’ which are enacted by international organizations, since the persons to which the code will be applied are not participating in the process.⁵⁵ In a way which is not very different, Pierre Trudel defined it as “the recourse to

⁵¹ Weinberg J. 1997, Rating the Net, <http://www.msen.com/~weinberg/rating.html>

⁵² *ibid.*

⁵³ Cranor L. F. & Resnick P., Technology Inventory, art. cit.

⁵⁴ See <http://www.w3.org/PICS/PICS-FAQ-980126.html>

⁵⁵ Pierre Van Ommeslaghe, L’*autorégulation*. Rapport de synthèse, in: *L’autorégulation*, Actes du Colloque organisé par l’A.D.Br. et le Centre de droit privé de l’Université libre de Bruxelles le 16 décembre 1992, Bruxelles, Ed. Buylant, 1995, pp. 233-274.

voluntary norms which are developed and accepted by those who participate in a determined (specific) activity.”⁵⁶

Our Corpus - Different Styles

We have gathered some 15 documents - codes or rules - which may be relatively well recognized as self-regulatory instruments of governance for the Internet to which we joined the 30 IFIP Codes that we had analyzed before.⁵⁷ Our collection shows the extreme diversity of the material which comes under the label ‘self-regulation’. We tried to classify the documents according to the Van Ommeslaghe’s classification but we were obliged to consider it as inapplicable.⁵⁸ The present list is more classified on themes or names.

The ‘Ten Commandments’ and the Netiquette rules

- The Ten Commandments of Computer Ethics, by the Computer Ethics Institute (CEI), Washington, D.C.; published in many places.⁵⁹
- Suggestion of Netiquette - Core Rules of Netiquette, Virginia Shea.⁶⁰
- The Net: User Guidelines and Netiquette, by Arlene H. Rinaldi.⁶¹
- Charter and Guidelines for news.admin.net-abuse.announce, Source: Newsgroups: news.admin.net-abuse.announce, 11 April 1995.
- One planet, One Net: Principles for the Internet Era, CPSR (Computer Professionals for Social Responsibility): still under discussion.⁶² (not analyzed)

Charters

- Cyberspace and the American Dream: A Magna Carta for the Knowledge Age, 1994, published by the Progress and Freedom Foundation (PFF).⁶³
- Online Magna Charta, Charta of Freedom for Information and Communication, ‘The Wartburg Charta’, 1997.⁶⁴
- The Intergovernmental Information Technology Leadership Consortium (Council for Excellence in Government) - Draft - Consortium Charter, 1997.⁶⁵

⁵⁶ Pierre Trudel, Les effets juridiques de l’autoréglementation, in: *Revue de Droit de l’Université de Sherbrooke*, 1989, vol. 19, nr. 2, p. 251, quoted by Olivier Hance, L’évolution de l’auto-réglementation dans les réseaux informatiques: Eléments pour la construction d’un modèle théorique, in: *Journal de Réflexion sur l’Informatique*, Namur, Août 1994, Nr. 31, pp. 25-31.

⁵⁷ J. Berleur and Marie d’Udekem-Gevers, Codes of Ethics Within IFIP and Other Computer Societies, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, J. Berleur & Kl. Brunnstein, Eds., Chapman & Hall, 1996, pp. 3-41.

⁵⁸ Pierre Van Ommeslaghe, L’autorégulation. Rapport de synthèse, art. cit. pp. 251 ff.

⁵⁹ See for instance: <http://www.fau.edu/rinaldi.net/index.htm> (July 1998)

⁶⁰ Virginia Shea, *Netiquette*, San Francisco: Albion Books, 1994 (See: *EDUCOM Review*, Vol. 29, Nr. 5, September/October 1994, pp. 58-62). See also: <http://www.educom.edu/web/pubs/review/reviewArticles/29558.html> (July 1998)

⁶¹ <http://www.fau.edu/rinaldi.net/index.htm> (July 1998)

⁶² In: *CPSR Newsletter*, Volume 15, N°4, Fall 1997.

See also: <http://www.cpsr.org/dox/program/nii/onenet.html> (July 1998)

⁶³ <http://www.pff.org/position.html> (July 1998)

⁶⁴ <http://www.lipsia.de/charta/> (July 1998)

⁶⁵ <http://www.excelgov.org/techcon/charter.htm> (July 1998)

Codes of Ethics and Conduct

- Codes (Standards/Guidelines) of Ethics (Practice/Conduct) of IFIP Computer Societies.⁶⁶

ISPs', SPA's Codes, 'Virtual communities' rules and others Codes of ISPs' (Internet Service Providers) Associations

- Internet Service Providers Association (ISPA-UK), Code of Practice, 1996.⁶⁷
- Internet Service Providers Association (ISPA-Belgium), Code of Conduct, 1998.⁶⁸
- Canadian Association of Internet Providers (CAIP), 1997.⁶⁹
- La Charte française de l'Internet, Proposition de Charte de l'Internet, Règles et usages des acteurs de l'Internet en France, 1997.⁷⁰
- La Charte de l'Internet proposée par la France à l'OCDE, Proposition française présentée à l'OCDE pour une Charte de coopération internationale sur Internet, 23 octobre 1996.⁷¹ (not analyzed)

'Virtual Communities'

- JANET Acceptable Use Policy, 1995.⁷²
- GeoCities Members Guidelines, and particularly GeoCities Page Content Guidelines and Member Terms of Service, 1998.⁷³

Others

- US SPA's (Software Publishers Association) Guidelines for Copyright Protection (previously called 'ISP Code of Conduct'), 1997.⁷⁴
- International Chamber of Commerce, Guidelines for ethical advertising on the Internet, 1998.⁷⁵

Most of them are short, maximum 2 A4 pages; but some are shorter than others; 10 commandments, 10 rules of Netiquette, 7 principles for the Internet era. Symbolic figures! And sometimes one stresses that it must be a 'portable' regulation: CPSR doesn't hesitate to launch its idea 'One planet, one net' on a book marker! It seems that that the shortness is a characteristic of such kind of documents, except when they are 'codes of practice'. But this shortness has, at least, to be combined with the content density!

⁶⁶ J. Berleur and Marie d'Udekem-Gevers, Codes of Ethics Within IFIP and Other Computer Societies, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, J. Berleur & Kl. Brunnstein, Eds., op. cit.

⁶⁷ <http://www.ispa.org.uk/codenew.html> (July 1998)

⁶⁸ <http://www.ispa.be> (July 1998)

⁶⁹ <http://www.caip.ca/caipcode.htm> (July 1998)

⁷⁰ <http://www.planete.net/code-internet/> (July 1998) (Translation "Proposition for an Internet charter, Rules and Courtesies of the Actors of the Internet in France, 1997", done by Dr. Victoria Steinberg, Foreign Languages Department, University of Tennessee, Chattanooga, USA).

⁷¹ <http://www.telecom.gouv.fr/francais/activ/techno/charteint.htm> (July 1998)

⁷² <http://www.ja.net/documents/use.html> (July 1998)

⁷³ <http://www.geocities.com/members/guidelines/> (July 1998)

⁷⁴ http://www.eff.org/pub/Legal/Cases/SPA_cases/spa_revised_isp.code (July 1998)

⁷⁵ http://www.iccwbo.org/Commissions/Marketing/Internet_Guidelines.html (July 1998)

A tentative analysis

The 'Ten Commandments' and the Netiquette rules

The first series of texts is a mix of prevention against what is called computer crime (for the *Ten Commandments*) and of kindness and fairness (for the *Netiquette* rules). Many of the rules governing Newsgroups, for instance the 'Charter for news.admin.net-abuse.announce', are worth being mentioned since they make explicit what is considered as "net-abuse", and which is spelled out, at least partially, in terms similar to those used in computer crime laws.⁷⁶

The categories of computer crime which were adopted by the Council of Europe in 1990 may fix our attention and cover the majority of the topics here suggested.⁷⁷ The Council of Europe recommended to have a *Minimum List*, which includes computer related fraud, computer related forgery, damage to computer data or programmes, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer programme, unauthorized reproduction of a topography, and an *Optional List* covering alteration of computer data or programmes, computer espionage, unauthorized use of a computer, and unauthorized use of a protected computer programme.

The Charters

'Cyberspace and the American Dream: A Magna Carta for the Knowledge Age' is a manifesto of the Progress and Freedom Foundation (PFF), in the spirit of the third wave of the Tofflers.⁷⁸ If we mention this 'Carta', it is only to notice the hot issues as they are seen by certain zealous propagandists: property rights necessary for the market, infrastructure ownership, dynamic competition on the Cyberspace marketplace and Schumpeter's 'creative destruction' with its winners and losers, customized and actionable knowledge for the Knowledge Age, hackers "vital for economic growth and trade leadership", ...

The 'Online Magna Charta, Charta of Freedom for Information and Communication, The Wartburg Charta' (1997), is no more than the previous one, a 'Charter'. It is a protesting reaction of Netizens when the US CompuServe provider blocked the access to 200 discussion fora under judiciary inquiry, in November 1995. It is a claim to the right to free speech and the freedom of opinion, information and communication, the right to 'a virtual home'.

The last 'charter' here mentioned is the 'Intergovernmental Information Technology Leadership Consortium Charter' which again does not fit into that category and is more a self-satisfactory statement promoting its own quality in the delivery of government services, in the economic growth, and in the citizen participation at all levels of the process of governance.

⁷⁶ I was told, in April 1998, by the former moderator, that this group does not exist anymore.

⁷⁷ Council of Europe, Computer-Related Crime, Recommendation N° R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems, Strasbourg, 1990. See also : Jay Bloombecker, Simplifying the US State and Federal Computer Crime Law Maze, in: *Transnational Data and Communications Report*, September/October 1994, pp. 6-8.

⁷⁸ Alvin and Heidi Toffler, *Creating a new civilization. The politics of the third wave*, Foreword by Newt Gingrich, Turner Publishing, Inc., Atlanta, 1995.

Codes of Ethics and Conduct

Codes of Ethics and/or Conduct of many computer societies, such as in IFIP, are not specific to the Internet, but their content is rather frequent in such a kind of self-regulation and so worth noticing.

The 'fields of reference' which have been considered by at least one third of the 30 codes of the IFIP national member societies which we have examined are as follows :

- Respect for the interests or rights of the people involved, for the prestige of the profession, for the interests or rights of the public, for the welfare, health of the public, and for the quality of life;
- Conscientiousness and honesty, acceptance of responsibility and integrity, respect for requirements or contracts or agreements, conscientious work, professional development and training , competence, effectiveness and work quality;
- Confidentiality, privacy in general and respect for property rights;
- Flow of information to involved parties, and information to the public;
- Respect for the code, for the law, and for IT and professional standards.

ISPs', SPA's Codes, 'Virtual communities' rules and others

Our collection of self-regulatory documents still include 4 Codes of Internet service providers associations, 2 'virtual communities' rules, 1 Software publishers association Guidelines for Copyright protection, and 1 International Chamber of Commerce Guidelines for ethical advertising on the Internet.

Codes of ISPs' Associations

The 'French Proposal of an Internet Charter' must be included in the category of ISPs' codes, more than in the charters' category. On the opposite, the 'US SPA's Guidelines for Copyright protection', although it was called earlier 'ISP Code of conduct', will be mentioned in our last category 'Others'. The French proposal - still a draft - is the most complete one, and also the longest: it is more than 12 pages long whilst the others are generally 2 pages. It seems also that in Europe, at least among the 10 EuroISPA members, there are only 2 having presently a code.⁷⁹ So, our collection contains, first, 4 codes of ISPs' Association: two Europeans (UK and Belgium), one Canadian, and the French draft.

The comparison regarding the people concerned and the country does not reveal great mysteries: the members of the association and the country where it is located! Let us just mention the CAIP's Code which stipulates that "it will cooperate with international organizations and law enforcement authorities ..." Procedures for enforcement are not very strong, and the commitment for reporting is weak.

As the topics are concerned, at the risk to be regarded as nationalist, let us take the most recent code, from Belgium. Except the French draft, it is the most complete and it includes most of the items of the others. It includes general commercial clauses insisting on legality and sincerity (services, products or advertising material), honesty (with clients; inform them of this existing code), personal data protection, publicity, and right information on prices.

⁷⁹ <http://www.euroispa.org/coc.html> (July 1998) A recent update (August 1999) brought the number of codes to 6, for 11 members.

These commercial clauses are spelled out in similar terms in the UK and Canadian documents. There are also special clauses on crime in the Belgian code: pay special attention for fighting against ‘illegal or dubious material’, but no capacity for controlling everything; they will assist public authorities, have special email address for complaints, and inform hotline about every illegal or harmful transaction: sex, pornography, paedophilia, racism, xenophobia, genocide denial, provocation or encouragement to criminal act, criminal association, gambling and lottery, drugs (“list is not closed”), ...

What the draft French Internet Charter seems to bring new in the scope is the creation of what is called an ‘Internet Council’, “an independent and unique body for self-regulation and mediation.” Its roles will include information and advice to actors and users, process of complaints, and participation in the international cooperation. The role is a bit larger than the ISPs associations. The Canadian association of Internet providers code resembles to the others, but one specific clause is worth mentioning: “CAIP members are committed to *public education* about Internet issues and technology (f.i. how to assign liability for content and network abuse, and help all Canadians understand the options available to all stakeholders).

‘Virtual Communities’

JANET is the well known UK education and research community network. We do not have here a real document of ‘self-regulation’, but an ‘acceptable use policy’, as it is most of the time called in Anglo-Saxon world.⁸⁰ But it contains rules which are typical not only of such academic community, but of many others: privacy protection, no harmful material, no computer crime (unauthorized access, no defaming, no infringement of copyright, corrupting or destroying other users' data, disrupting the work of others, other misuse of JANET or networked resources, such as the introduction of ‘viruses’, etc.), and also some rules of usual Netiquette such as: “Do not use JANET for deliberate activities such as wasting staff effort or networked resources, (...) in a way that denies service to others, ...

JANET acceptable use policy is a very temperate and sober community code when compared to the GeoCities Guidelines. GeoCities could be classified among the ISP, but it looks also like a big community - ‘more than 2 million GeoCitizens’ from all the world, located in some 40 ‘Neighborhoods’ - common interest communities.

Regarding the illegal or harmful material, the rules do not differ very much from what we have read until now. “Refrain from using free Personal Home Page or GeoCities Chat and Forum session for: material containing nudity or pornographic material; material grossly offensive to the online community, including blatant expressions of bigotry, prejudice, racism, hatred, or profanity; material that exploits children under 18 years of age; restricted or password-only access pages, or hidden pages or images (...).”

There are other interesting clauses. “Refrain from: instructional information about illegal activities, physical harm or injury against any group or individual, or any act of cruelty to animals; defaming any person or group; for commercial purposes (...); using page (or directory) as storage for remote loading or as a door or signpost to another home page.”

The list includes a clause which is nearly the copy of one from the US SPA Guidelines for Copyright Protection, as we shall see: “refrain from using your home page for acts of

⁸⁰ See John W. Corliss, Policies of Acceptable Use at Educational and Research Institutions, in: *Ethics of Computing: Codes, Spaces for Discussion and Law*, J. Berleur & Kl. Brunnstein, Eds., op. cit. pp. 61-70.

copyright, trademark, patent, trade secret or other intellectual property infringement, including but not limited to offering pirated computer programs or links to such programs, information used to circumvent manufacturer-installed copy-protect devices, including serial or registration numbers for software programs, or any type of cracker utilities (this also includes files which are solely intended for game emulation).”

Then it goes on with: “Refrain from: violating Internet standards for the purpose of promoting your home page; hyperlinking to content not allowed in GeoCities; gathering personally identifiable information for commercial or unlawful purposes; posting or disclosing any personally identifiable information belonging to children. [Kids: For your safety, do not put your real name, address, phone number, e-mail or other information like that on your webpage or give it to strangers.]”

This rather long list is completed by an explicit sentence: “GeoCities does not actively monitor the content of Personal Home Pages but will investigate complaints of violation of these guidelines.

Others

We have finally collected two specific Guidelines, because they are ‘sectoral’ and linked to the Internet.

The first one, the Guidelines of the US SPA are in a way curious, because they have been developed by SPA for server operators who do not seem “to participate in the activity”, to quote the definition of self-regulation by Pierre Trudel: the real actors on whom self-regulation is here imposed are the subscribers. The question was very controversial: SPA suited small ISPs, but the case was dropped.⁸¹ Amusingly, when writing this paper, we found a ‘Hotnews’ ‘Dutch ISPs Refuse to Squeal on Software Pirates’: “Dutch Internet service providers World Access/Planet Internet, XS4All and Euronet have said they will not check their systems for advertisements by software pirates, even though the Business Software Alliance (BSA), an organization of software distributors, holds the providers responsible for the majority of software piracy over the Internet in the Netherlands.”⁸² The subject is surely hot and on the agenda of many organizations, as well as the general problem of intellectual property right.⁸³

The Guidelines of ICC on Advertising and Marketing on the Internet are surely worth seeing, since we are here also in a very sensitive domain. The privacy protectors and the anti-spamming leagues will surely react to such guidelines. Problems which are here treated are: legality, honesty, social responsibility, clear information to the users, use of personal data (with a right to opt-out), right to access his/her own data, no unsolicited commercial message (when indicated), special clauses for advertising to children, and respect for potential audiences: pornography, violence, racism, sexism, ...

⁸¹ Electronic Frontier Foundation (EFF), Software Publishers Association vs. ISPs - suits dropped, ‘Code of Conduct’ critiqued [Dec. 6, 1996], <http://www.eff.org/pub/Censorship/HTML/hot.html#cda> (July 1998)

⁸² Dutch ISPs Refuse to Squeal on Software Pirates, <http://www.best.be/hotnews.CFM?DPPRESS=743> (July 10, 1998).

⁸³ Robin Mansell and W. Edward Steinmueller, Intellectual Property Rights: Competing Interests on the Internet, in *Communications and Strategies*, IDATE-Montpellier, n° 30, 2nd Quarter 1998, pp. 173-197.

Self-Regulation : First Results

What could be considered in some way as a tedious analysis reveals repetitions and a rather convergent final result. Some ‘issues’, if not ‘categories’, emerge:

- fairness and kindness: Netiquette, ISPs, ICC
- respect, honesty, competence, sincerity, right information, ...: Codes, ISPs, ICC
- privacy (and deriving rights such as right to know about his/her own data): nearly all
- computer crime: Ten Commandments, Net-abuse administration, Virtual communities, Janet, ICC
- intellectual property right, copyright, trademark, patent, ...: GeoCities, PFF Carta, US SPA
- free speech, right to information and communication: Wartburg, French Charta
- illegal, dubious, harmful material: ISPs, GeoCities, ICC
- etc.

We must say our disappointment about the other features of our analysis: people involved and concerned, places where self-regulation is applicable, rules for enforcement. It looks like the reign of vagueness.

About enforcement and procedures, without doubt, we are in a relatively recent situation: the texts we have examined do not go back further than 1994-1995. Moreover, as most often, organizations do not like to report on complaints which could reveal a weakness in their security system, for instance. This means that we shall have difficulties to evaluate the functioning of the procedures, when they exist. We can just regret that some organizations explicitly state that they cannot commit themselves in controlling what they have on their servers.

This means that, if the topics and issues appear relatively clearly, the main concern, in terms of governance, reveals that we have to make further decisive progress. We could also add that the real problem with such codes is not that they exist, but that in some pages they try to cover what the law needs many well crafted numerous articles for!

The Internet : The Role of the law. Two new legal issues

The problem of the regulation of the Internet could be solved in different ways. The law is one of them. But, because of the particular nature of this new medium, and especially the fact that it allows to exercise a lot of different fundamental freedoms (like the freedom of expression, the freedom of information, etc.) important ethical choices have to be made in order to conciliate all interests.

To give a better idea of these ethical choices, we will analyze the regulation chosen in two different topics: the protection of privacy and the protection of copyrights.

The Protection of Privacy

Different choices have been made in USA and in the European Union. These choices could be explained in an economical point of view. On the one hand, we have the United States of America whose economical tendency is liberalism, which means that the market

should be let free to solve as much issues as possible. On the other, the European Union which has chosen to regulate.

The Choice Made in the United States

In July 1997 the Clinton's Administration published a paper entitled : "Framework for global electronic commerce" in which different principles were developed from which three are relevant for our purpose.⁸⁴

First of all "the private sector should lead" and consequently, the government will encourage industry self-regulation and the private sector participation in the making of standards or collective agreements. Secondly, "Governments should avoid undue restrictions on electronic commerce". Thirdly, "where governmental involvement is needed, its aim should be to support predictable, minimalist, consistent and simple legal environment for commerce" which means that the Governments plans to set up only decentralized or contractual model of law rather than a legal environment base "on top-down regulation".

The choice of the federal administration was clearly in favour of self-regulation. But in 1998, a poll taken by *Business Week* revealed that a lot of citizens refused to go online because of privacy concerns. The efforts of the companies to set up adequate privacy protection seemed not to be convincing. It is why in July 1998, the Federal Trade Commission made the following declaration : "Unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of the year, additional governmental authority would be appropriate and necessary."⁸⁵

One month later, the Federal Trade Commission charged the company GeoCities, one of the most popular sites on the World Wide Web, of misrepresenting the purposes for which it was collecting personal identifying information from children and adults.⁸⁶ A few days later, the GeoCities' shares lost more than 20 percents. And that can be considered as a mirror of the growing awareness "that Internet privacy protection can have an enormous impact on a company's bottom line."⁸⁷

The Choice Made in Europe

The legal policy in the European Union has clearly been a regulatory policy. A general directive was issued in 1995 and set up different rights such as the right of access or the right to object.⁸⁸

The general directive speaks also about the self-regulation, and one article is really interesting to understand the place the self-regulation should take (mostly the Codes of Conduct). The article provides that: "The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account

⁸⁴ <http://www.ecommerce.gov/framework.htm>

⁸⁵ <http://www.wired.com/news/news/politics/privacy/story/13895.html>

⁸⁶ <http://www.ftc.gov/opa/1998/9808/geocitie.htm>

⁸⁷ Reuters 17/08/1998.

⁸⁸ Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L 281, 23.11.1995, p.31 (hereinafter general directive). (Right of access: see article 12; right to object, see article 14)

of the specific features of the various sectors”.⁸⁹ The Commission seemed to consider the Code of Conduct only as a supplement to the law, nothing more.

This article also creates the possibility for trade associations and other bodies representing other categories of controllers to submit the code they have drawn up to the opinion of the national authority. The Directive suggests that the Member States should make provision for this authority to ascertain whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to the Directive.⁹⁰

But at this point of the debate we have only compared the choice made in the United States and in the European Union. It would be interesting to join them face to face. The first feature of this confrontation is the article 25 of the European Directive, which provides that : “the member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the directive, the third country in question ensures *an adequate level of protection*” the second paragraph of the article gives more details about the assessment of the level of protection saying that “particular considerations shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country” . At that moment the level of protection in the USA has been considered as inadequate. But the problem is that the Directive will have direct effect in October 1998. Therefore, US and EU officials are meeting to discuss ways of avoiding a potential impediment to electronic commerce trading between the two continents.

The problem is now: How to solve this conflict? Because both parties will stay on their positions. A solution could may be found in the article 26.2 of the European Directive which creates an exception where the controllers adduce adequate safeguards with respect for the protection of privacy specifying that such safeguards may in particular result from appropriate contractual clauses. So the solution could be the creation of standard contracts which would be used for each transborder data flows to third countries.

In 1997, the Commission issued a second Directive on privacy, particularly focused on the telecommunications.⁹¹ This Directive gives several rights to the consumer with regards to the use of telecommunications, which can be made with a commercial purpose. For example, article 10 says that a subscriber must be provided, free of charges, with the possibility to stop automatic call forwarding by a third party to his or her terminal. These calling systems include the fax transmission, so doing; the Directive provides a solution to the problem of commercial harassment.

In conclusion, we can observe that the process used in the European Union is exactly the contrary to the one adopted in the USA. In a first step, the Clinton’s Administration had given the priority to the self-regulation. But recently they have faced different abuses of the market due to the lack of regulation. They probably will come to the decision to write a law. But something remains surprising. It is the fact that the financial market has started to consider the

⁸⁹ Article 27 §1.

⁹⁰ Article 27 2 al. 2.

⁹¹ Directive 97/66/EC of the European Parliament and of the Council of the 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ 1998 L24/1.

protection of Privacy as a criterion to evaluate a company carrying business in electronic commerce. Therefore it could be considered that a change of the way to regulate privacy in the USA would be the result of an economical choice more than of an ethical one.

On the opposite, the European union started directly with a directive whose purpose was, among others, to ensure a high level of protection to the right recognized in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁹² The choice of the Commission was to enforce that ethical value with a Directive but with a possibility to use self-regulation as a complement. It could be asked which of those two process is the most efficient. The answer could be none of them because they both try to stay between the over-regulation and the legal emptiness knowing that each of them is really close to the farthest utmost point.

The Protection of Copyrights, the Competition between Law and Technology

Opposite to the privacy domain, the field of copyright has been regulated strongly in the USA and in the European Union. The ethical choice has been done in favour of a real protection of the rightholders. But, new questions arise now with the coming out of technical systems of protection. These systems are capable of managing the access to the works.

Furthermore, a proposal for Directive on copyright and related rights in the information society would require Member States “to provide adequate legal protection against any activities, including the manufacture or distribution of devices or the performance of services, which would enable or facilitate the circumvention without authority of effective technological measures designed to protect copyrights and related rights.”⁹³

This position of the Commission is the starting point of different considerations. First of all, the danger is that such an Electronic Copyright Management System (ECMS) could manage the access to works, which are not protected anymore by copyrights. Which might, according to different authors, “result in appropriation of public domain, which has to remain freely accessible to the general public.”⁹⁴

Furthermore, the technology seems to offer a better protection than the copyrights themselves, and one could ask if that technology will not cause the “death of the copyrights” in the virtual world? This remark could be found excessive but something is certain, the spirit of the protection by the copyright is changing. Before the protection was an *a posteriori* one the copyright was invoked after the infringement. Now, to prevent the ECMS to violate the right of information of the public, it becomes necessary to decide *a priori* which works are protected and which are not.

It is interesting to note that the emergence of the new information technologies could be regulated by three different instruments : first of all the law which has the advantage to be effective and possibly enforced by a court order. But, the law has also weaknesses such as its

⁹² Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L 281, 23.11.1995, p.31, whereas (10).

⁹³ <http://europa.eu.int/comm/dg15/en/intprop/intprop/1100.htm> (comments on article 6).

⁹⁴ Severine Dusollier, “Legal aspects of Electronic Rights Management Systems (ERMS)”, p.6. (to be published)

general character which does not help when practical details have to be solved. The second way to regulate is the self-regulation. This way is generally chosen in sectors where the connections between the actors are very strong like for example in the financial world. The self-regulation has an effectiveness when it is the commercial advantage of the actors to comply with. If it is not, it is really difficult to imagine that such a regulation could have any possibility to be enforced.

A third and new way to regulate is the technology which can integrate the requirements of the law and enforce them by technological ways. The danger resides in the following question: “Who is entitled to write the standards governing the machine?” Because if only an oligarchy decides of the rules to be implemented by the machine they give to the law their own interpretation and sometimes bypass completely the philosophy of the rule. If, like some authors said “the answer to the machine is the machine”, the user has to remain the master and may not become the slave ...

Conclusion

We may be short. Two main conclusions are obvious and could be considered at least as a provisional agreement and allow us to focus on newer issues.

First, there is a general agreement on the ethical issues as they are covered either by the technical means, or by self-regulation, and partially at least by the law. Privacy (and deriving rights such as right to know about his/her own data); computer crime; intellectual property right, copyright, trademark, patent; free speech, right to information and communication; fight against hatred speech, racism, and against sectarianism; pornographic, illegal, dubious or harmful material; etc. All these issues are rather frequently mentioned.

Second, within the ways those issues are solved, or at least approached, there are also ethical choices to be clarified. Who is setting the labeling vocabulary and the criteria for assigning labels, who is rating the web sites ? Who is establishing the filtering criteria ? Those questions that we have raised about the technical means show us that there are social and ethical choices. As we have seen there are also ethical and social choices in the ways privacy may, for instance, be protected. Or it may be that a technical choice deregulates the legal means - what is also an ethical and social choice!

Ethics is not out of scope in the governance of the Internet, and plays its role. Therefore, as it was suggested during the recent IFIP-TC9 international conference on Human Choice and computers, we must “care about the net” instead of fearing it, play a role in a more face-to-face way (E. Lévinas); in other words we must devote ourselves to “netmaking” more than to “networking” and we have to *create* an ethical community. Others were suggesting to strive to develop cross-cultural values to the service of great causes such as reducing violence and promoting peace. Or, to develop principles of governance which include social responsibility. Social dialogue, cultural dialogue, social responsibility are not only important words: they must be in the forefront of our action to create human networks in the age of globalization.