Concerns from a European user-empowerment perspective relating to Internet content

d'Udekem-Gevers, Marie; Poullet, Yves

Published in:
Communications & strategies

Publication date:
2001

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

Concerns from a European User-Empowerment Perspective relating to Internet Content (*)

Marie d'UDEKEM-GEVERS
Institut d'Informatique,
University of Namur, Belgium

Yves POULLET
Centre de Recherche Informatique et Droit (CRID),
University of Namur, Belgium

■ How to Regulate Internet and what to Regulate?

How to regulate the Internet

The debate over Internet content regulation is a heated one. What is the best way to regulate? There exist three web regulation paradigms: self-regulation, Government regulation and co-regulation (POULLET, 2000). Self-regulation contrasts with traditional public regulation. The OECD inter-ministerial Conference of Ottawa held in October 1999 proposed a third way: 'co-regulation' or an 'effective mix' between self-regulation and public intervention. This third approach seems to have received great support over the last two years.

(*) This paper has been produced thanks to financial support of the Belgian 'Federal Office for Scientific, Technical and Cultural Affairs' (OSTC), within the framework of the programme *Pôles d'Attraction Interuniversitaires (PAI IV)*. It was also carried out within the framework of the Internet Action Plan World Wide Web Safe Surfing Service funded, in part, by the European Community under the contract IAP PROJECT 26653-3W3S. The authors thank N. CONDON for having corrected their English text.

Self-regulation (or private regulation)

Self-regulation is a private norm, i.e. a norm enacted by private parties. It therefore marks a contrast with a public or governmental norm which is enacted by public authorities within the limits and based on their 'constitutional' competencies i.e. a law. TRUDEL (1989) defines the concept of self-regulation as "norms voluntarily developed and accepted by those who take part in an activity".

A report prepared for the OECD (GIDARI, 1998) stated "while there is a broad consensus that self regulation of the Internet is critical to its future growth, there is little consensus about how to achieve and to implement a self-regulatory regime". Self-regulation is a word and a myth: the concept is presented as an adequate solution born of the disintegration of the traditional "national sovereignty" paradigm (REIDENBERG, 1996) on which the traditional regulatory powers given to constitutional State authority were founded.

As regards these private sources, we may observe that self-regulation is not limited to very isolated norms but, rather, increasingly encompasses a set of structured norms included within codes of conduct or codes of practice (1), and provides not only the content but also the means to enforce these rules. The actors themselves have developed means to ensure that the self-regulatory code passes from the letter to the act.

The typical sanctions in the regulation of a network, such as disconnection and 'flaming', are strangely reminiscent of vigilante justice. New means of enforcement have arisen over the last few years, triggered by the battle against illegal or harmful content on Internet.

The hotlines set up by certain codes of conduct, to enable the condemnation of activities contrary to that code, represent another example of the means deployed to ensure adherence to network discipline. Furthermore, there are different initiatives for the creation of 'virtual magistrates' (KATSCH, 1996 and PERRITT, 1996), on-line arbitrators or mediators who are authorised to adjudicate conflicts arising out of network use, whether they be issues of defamation, violation of privacy or non-adherence to a newsgroup's rules. Such Alternative Dispute Resolution (ADR) (2) mechanisms have been recently promoted by the European

(1) See notably Internet Industry Association, December 1999.
(2) The acronym ADR covers all methods of resolving conflicts or disputes resulting from electronic transactions operated by independent bodies other than official courts. This phenomenon is greatly encouraged as regards the solution of conflicts over domain names but is also proposed for solving disputes in other areas (consumer protection, privacy, etc.). The European Parliament and Council 'directive on electronic commerce' (2000) has officially requested that the Member States acknowledges the creation and the legal values of these

directive on certain legal aspects of Electronic Commerce in the internal Market (3).

Some systems, such as the quality labelling (LOUVEAUX, POULLET & SALAÜN, 1999) mechanisms which both guarantee and inform the user of the quality of the service being offered (such as the 'privacy friendly' label or the label relating to journalistic information websites that state respect of the press code), are of greater interest. Naturally, the value of such a certification depends on the quality of the certifying body that defines, issues and controls it.

Thus, we can see that private regulatory sources establish their own mechanisms for expressing the rules, controlling their application and, ultimately, for sanctioning violations; in certain cases, the sanctions are imposed by their own 'magistrates'.

Government regulation (or public regulation)

Public regulation can be the responsibility of a State or an international authority.

Currently, several countries have implemented public government regulation of Internet content. Singapore, for example, is a case in point as noted in the following official text (Singapore Broadcasting Authority –SBA–, 1996):

"1. The Singapore Broadcasting Authority Act (Cap. 297) makes it the duty of the Singapore Broadcasting Authority to ensure that nothing is included in any broadcasting service which is against public interest or order, national harmony or which offends against good taste or decency. This Code (4) of Practice has been produced by the Singapore Broadcasting Authority for this purpose.
2. All Internet Service Providers and Internet Content Providers licensed under the Singapore Broadcasting Authority (Class Licence) Notification 1996 are required to comply with this Code of Practice. Under the Singapore Broadcasting Authority Act, the Authority has the power to impose sanctions, including fines, on licensees who contravene this Code of Practice."

initiatives under certain conditions as regards the independence of the "judges", the procedure followed before these courts and the transparency of their decisions.
(3) Cf. Article 17 of the European Parliament and Council 'directive on electronic commerce' (2000).
(4) This use of the words 'code of practice' can be considered improper because this code is not provided by the professionals themselves but by SBA.

SBA (1999) considered that this is a "light-touch enforcement approach... which means that an offender will be given a chance to rectify the breach before SBA takes any action". It must be underlined that the Singaporean model provides a reference to a Code of Practice which was discussed by the Broadcasting Authority and all interested parties before being enacted (5).

On the other hand, the information superhighway's international aspect drives States to search world-wide for models for developing legislation, or to establish co-operation among national authorities (FRYDMAN, 1997). Through international conventions(6), bodies (7), treaties for policy co-operation amongst States engaged in the fight against cyber-crime and the draft for an International Internet Co-operation Charter presented by France on October 1996 (8) to the OECD, a number of public initiatives have taken on the State's traditional role of protecting and safeguarding individual rights and public interest. The Council of Europe published on October 2000 a Draft Convention on Cyber-crime (9). Some have gone so far as to suggest the creation of an "International Cyberspace Authority", reacting to movements for the emancipation of Internet law and to the increasing power of private norms. The "new world order for global communications" (10) promoted by the former European Commissioner, M. BANGEMANN (1997a & 1997b), stressed the importance of setting up this global authority and fixing global rules for e-commerce.

But, when such a solution is envisaged, the operational complexity of international forums and their deficit of democratic discussions and liability are frequently invoked. Nevertheless, due to the international dimension of the network of networks and the increasing need to define common rules, their presence is growing steadily.

(5) Compare with the Australian co-regulatory model where the Code of Practice is generated by the sector itself but must be approved by the Australian Broadcasting Authority (see infra).
(6) Such as those of the UNO, UIT, WTO, WIPO, OECD.
(7) Such as the G7.
(8) See 'Charte de l'Internet, 1996'.
(9) The Council of Europe in co-operation with the Italian *National Direction Antimafia* has organised a first pan-European Conference about the "Defence of the Society *vis-à-vis* the organised criminality", Caserta, 8-10 sept. 2000.
(10) The Bangemann's suggestion for an 'international charter for global communications' underlining the need for a strengthened international co-operation was made in September 1997. Since then, the European Commission has issued a communication (1998) on the "The need for strengthened International Co-ordination" which aims both to provide a business dialog [which should lead to remove all technical (including legal) barriers to electronic commerce] and to ensure the political support and leadership in order to ensure a democratic legitimacy.

'Co-regulation' (or 'joint regulation' or 'effective mix of public & private regulations')

The OECD Ministerial Conference on Electronic Commerce, held in Ottawa on 7-9 October 1998, was the scene of in-depth discussion on the idea of combining the two previous regulatory approaches in a co-regulatory effort of both private and public partners. The central idea being that it would be impossible to regulate the Internet effectively if private and public bodies do not combine their efforts. Still more recently, the World Summit for Regulators (11) pleaded clearly for a co-regulation.

So public regulation or State intervention are viewed both as a boost to self-regulatory techniques (see e.g. the initiative of the Dutch Ministry of Economy aimed at setting up a discussion platform which will lead to a code of conduct for electronic commerce negotiated entirely between private partners) and as a means for guaranteeing the effective sanctions of private regulations – see, for instance, the US Privacy Safe Harbor Principles (POULLET, June 2000) whose efficiency is guaranteed by the possible intervention of the Federal Trade Commission, which is a public juridical institution responsible for protecting the market against false and misleading statements, specifically in a case where a company has not respected the code of conduct to which it has declared to adhere. In that context, the two types of legal systems are placed on a more or less equal footing and a fixed division between the competencies of the first and the second ones is largely set according to what is known as the 'subsidiarity principle'.

As regards the division of responsibilities between the public and private regulatory intervention, we see the subsidiarity principle as an hermeneutic key principle used to fix the boundaries of the various regulatory techniques and bodies, including the self-regulatory ones (12). In other words,

(11) This summit was organised by the Unesco in co-operation with the Association of National Audiovisual Authority, November 30th and December 1st 1999, Paris.
(12) The subsidiarity principle has been asserted by the European Union in the context of the Maastricht Treaty and by the Council of Europe (see the Council of Europe Recommendation n° R (95) 19 about the implementation of the subsidiarity principle). This principle may have two different meanings. The first, is the assertion that local solutions are still needed and must even be preferred to international or global solutions insofar as the latter have to procure the general framework wherein these local solutions will take place and interoperate. From our point of view, local solutions, that means regional (from a geographical point of view) or sectorial, are the best way to take into account the cultural or business peculiarities of each situation and to develop adequate solutions. Otherwise, the regulations will be reduced to the enumeration of very vague and broad common principles.
The second meaning of the concept envisages the subsidiarity principle as a way to validate and fix the limits of the coexistence between the traditional regulatory model, the legislative one and the more 'modern' one : self-regulation. In our opinion, certain concerns might be more appropriately addressed by the selfregulatory solutions than by legislative ones.

everything you can fix by self-regulatory solutions must be fixed by self-regulatory solutions.

In February 2001, Liikanen, a Member of the EC responsible for Enterprise & the Information Society, declared:

"I consider that these approaches are a real alternative to traditional forms of regulation... It implies sharing of responsibilities through negotiated agreements between public and private partners... It implies self-regulation and [public] regulation being bound, linked and working together, so that they can mutually reinforce each other."

The co-operation and dialogue between private and public regulations are now usually considered (13) to be the best way to effectively ensure public interest objectives, with full respect for the balance embedded in our legislation and international Conventions. This is why we might consider co-regulation as integrated effective mix between public and private regulation.

We will return below to the concept of co-regulation to try to analyse the various levels of action and the various roles to be played respectively by public and private sectors. We will also give our opinion on these roles.

What to regulate

"There exists a whole range of rules which limit for different reasons the use and distribution of a certain content [e.g. child pornography]. The infringement of these rules lead to the 'illegality' of the content." (COM(96) 487 final p. 10)

On the other hand, "various types of material may offend the values and feelings of other persons: content expressing political opinions, religious beliefs or views on racial matters etc." (COM(96) 487 final p. 11). This kind of content is called 'harmful'.

Both illegal and harmful content has to be controlled on the Internet. Of course, "these different categories of content pose radically different issues of principle and call for very different legal and technological responses." (COM(96) 487 final p. 10).

(13) The Australian regulatory framework set up by the Broadcasting Services Act 1992 recently revised in 1999 may be considered as a model of this third approach. We will return below to this Australian approach.

■ Main European Union Official Texts relating to Internet Content Regulation

Before any discussion, let us thus recall several relevant excerpts from the main European Union official texts regarding illegal and harmful content on the Internet, and on the protection of minors and human dignity. On the one hand, for each text, we have pinpointed the main elements. On the other hand, we emphasised the evolution of these successive texts as regards the responsibilities for controlling Internet content.

The initial trend (before 1998): supporting private sector leadership

The first major texts from the Commission dealing with Internet content regulation are entitled respectively 'Green paper on the protection of minors and human dignity in audio-visual and information services' (COM(96) 483) and 'Illegal and harmful content on the Internet' (COM(96) 487 final). According to the first text (p. 24):

"The various industries concerned have a key role to play in developing and implementing solutions to the problem of protecting minors and human dignity... The main tasks which industry should work on are:
- drawing up a code of conduct...
- identifying areas where there may be a need for common standards on the labelling material;
- promoting the PICS standard or equivalent systems..."

Thus the European texts unambiguously support the leadership of the private sector (as in the case of the US (14). But these texts from the Commission also add important nuances and are quite different from US texts when speaking about cultural diversity:

"What is considered to be harmful depends on cultural differences. Each country may reach its own conclusion in defining the borderline between what is permissible and not permissible. It is therefore indispensable that international initiatives take into account different ethical standards in different countries..." (COM(96) 487 final p. 11).

(14) The President's Working Group on Unlawful Conduct on the Internet (2000) is still advocating this strong private sector leadership in the development of cyber-ethics to help, protect and empower internet users.

The second trend (1998-1999): encouraging private-public co-operation

Another important text is the Council Recommendation of 24 September, 1998 "on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity" (15). This text recommends (see p. 50):

"- the encouragement of the participation of relevant parties (such as users, consumers, business and public authorities)
- the establishment of a national framework for self-regulation by operators of on-line services... "

Let us underline that this text marks an evolution (16) in comparison with previous ones : self-regulation is no longer solely in the hands of the private sector. Public regulation is fixing the context of this self-regulation and the conditions of self-regulation legitimacy which must be set up, drafted, implemented and evaluated by all actors concerned by this regulation. Thus the industry will have to work alongside consumer watchdogs, liberties' associations, privacy authorities and, clearly, with official authorities in charge of criminal prosecution.

In the same vein as this Council Recommendation, let us note the European Parliament and Council Decision N° 276/1999/EC of 25 January, 1999 "adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks":

"The action plan has the objective of promoting safer use of the Internet and of encouraging, at European level, an environment favourable to the development of the Internet industry."

Its financial framework (EUR 25 million) supports four action lines, including:
- creating a safer environment (notably by encouraging self-regulation and codes of conduct),
- developing filtering and rating systems (demonstrating the benefits of filtering and rating and also facilitating international agreement on rating systems).

(15) It is worth noting that, according to the title of the recommendation, the competition between information services providers is invoked by the European Union authorities as the argument to uniformly regulate the Internet service content. The main concern of these authorities was to avoid any national regulatory approach since various regulatory ways would have created barriers against a unique internal European market.
(16) In US, the same evolution is clearly visible in a recent speech by the US Attorney General RENO (2000): "While law enforcement alone can't solve the cyberproblem, any effective strategy must involve us all."

Latest trend (from 2000): giving more investigative power to the state but limiting Internet provider liability

The Council decision to combat child pornography on the Internet adopted on May 29, 2000, following a Parliamentary report prepared by the Citizen's Freedoms and rights Committee based on an Austrian initiative, inaugurates a third trend granting more investigative powers to the official authorities. The main purpose of this decision is to reinforce the duties of the private bodies to work together with public authorities. Thus, certain measures are proposed to encourage Internet users to inform authorities of suspected distribution of child pornography material on the Internet, to force IAPs and other Information Society Service Providers to retain traffic-related data so that the data can be made available for inspection by criminal authorities (17); to check the identity of persons who obtain an e-mail address. The Council decision foresees the creation of a sex offenders' register accessible to all Member States, and of permanent points of contact to ensure timely and effective responses to child pornography offences. This increasing scope of duty for a large number of information services providers (not only the Internet Access Providers or hosting services but also the certification authorities, the trusted third parties or key recovery agents) to co-operate might be viewed as a compensation for the legitimate use of cryptography and other anonymity techniques in order to create a proper balance between free expression and privacy principles requirements and the public security needs. On 2 October, 2000, the Council of Europe published a draft convention on Cybercrime (18), which includes this duty to co-operate.

The adoption of the European Parliament and Council E-Commerce Directive of 8 June, 2000 should also be recalled here. Article 15 of this Directive states as a general principle that Member States may not impose on intermediaries a general obligation to monitor third party information they transmit, distribute or store. Furthermore, articles 12 and ff. recognise, in favour of specified online intermediary actors, a limited (both criminal and civil) liability and exclude any liability in cases where they are not aware of facts or circumstances which would have made the illegal activity apparent.

(17) National legislations have already expressly imposed this obligation : e.g. the Belgian Bill on computer crime currently being discussed by the Senate (Bill n° 214) has imposed this retention of traffic-related data for a maximum period of 12 months. The European Privacy Protection Authorities have condemned this measure which is disproportionate to public interests requirements and creates a risk of general surveillance of the population.
(18) This draft has been submitted for public discussion. See the Council of Europe Recommendation R (95) 13, concerning problems of criminal procedural law connected with Information Technology.

These important provisions constitute a legislative response to the concerns expressed by Internet actors [19] that ISPs should not be held liable in the case of illegal or harmful content unless they were aware of the infringement. They are considered by the European Union as a clear guarantee that there will not be a disproportionate restriction to freedom of expression, which is recognised as a pillar of the European Union and Market.

■ Players and Considerations of Internet Content Regulation

Players of Internet content regulation

Actors implicated in Internet content regulation are numerous, with providers on the one hand this regulation's customers, on the other [20].

Among the providers, several are 'traditional' in the Internet domain: Internet access providers (IAP), who offer access to Internet and its basic services (e-mail, web, news), Internet service providers (ISP), who offer complementary services (including hosting [21]); telecommunication companies (including network operators), multi-media and content providers (e.g. media and publishers).

The other providers are more recent arrivals on the market, and deal with the new products and services specifically relating to the control (i.e. filtering) of Internet content: filtering products manufacturers, labelling (i.e. assigning label) services (specific or additional activities) and people in charge of setting criteria for assigning labels. The list of this type of player will continue to grow and, in future, will include: label distribution services, bodies in charge of setting filtering criteria (i.e. customising) and, possibly, services dedicated to installing/running filtering software (see the 6 roles implicated by any filtering software according to RESNIC, 1998).

(19) These concerns, in particular, are picked up again by the Bertelsmann Foundation (see below) memorandum of 1999 (pp. 10 and 12).
(20) Another typology of the players can found in MATHONET et al. 1999, vol. 1 p. 13-29.
(21) They are, in this case, called 'web host providers'.

And, last but not least in the list of players, there are the Internet content regulation services' customers i.e. people or bodies in charge of the control itself: for example, parents, teachers, libraries in the case of harmful content and, for example, national security agencies or judicial powers (computer crime unit) searching for illegal data and activities.

Considerations of Internet content regulation

Several levels (see table 1) must be taken into consideration in the analysis of Internet regulation.

The first is economic and includes two sub-levels.

The first sub-level deals with the individual providers outlined above Indeed, selling new products or services related to the Internet content control might interest some traditional providers. Furthermore, content providers or ISPs might consider that a quality label gained by the use or the offer of these filtering or rating systems might serve as a helpful sales argument when marketing of their products.

Another economic dimension should not be underestimated: the recent judgements against web host providers who have hosted illegal web sites (JULIA-BARCELO & KOELHMAN, 2000) have fostered increasing fear among providers over the economic consequences of these decisions and have pushed them to seek adapted solutions (including the use of techniques selecting or at least scanning the content) to be made available to their customers.

At a more macroeconomic sub-level, the case of the Internet Content Rating Association (ICRA) [22] makes clear that the 'world's best known Internet and communications companies' are greatly interested in joining to try to control Internet regulation.

(22) ICRA associates the Bertelsmann Foundation, with among others, AOL Europe, British Telecom, Cable & Wireless, THUS, Deutsche Telekom Online Service, Electric Network Consortium Japan, EuroISPA (Internet Services Provider Association), IBM, Internet Watch Foundation, Microsoft, Software and Information Industries Association, UUNET. It "was formed in April 1999 as an independent, non-profit organisation. [Its] mission is to develop, implement and manage an internationally acceptable voluntary self-rating system which provides Internet users world wide with the choice to limit access to content they consider harmful, especially to children".

Given the growing economic importance of the Internet phenomenon, there is a risk that financial considerations of Internet regulation become the most important and somewhat eclipse the others.

The highest level (see table 1) deals with ethical considerations. Which values do we consider of public interest and do we want to promote? In the framework of Internet regulation, protection of minors (against illicit messages and harmful content), respect for personal values, respect for cultural diversity and free speech, respect for the anonymity on Internet which is considered as a tool for ensuring this freedom of expression (JULIA-BARCELO & KOELHMAN, 2000), can be mentioned. It has become increasingly clear that the various stated values conflict with one other, e.g. the freedom of expression principle will clearly restrict any forms of control over the web sites, control which might be justified for reason of protection of minors. In case of value conflict, how do we prioritise? The key, then, is to strike an appropriate balance between these contradictory values. This is clearly formulated in the following central question addressed by the (COPA) Commission on Child Protection (2000, p. 13):

"What are the most effective means of serving the public's interest in protecting children online that have the least potential adverse impacts on protected adult speech?"

When ethical choices have been made, it is time for socio-political choices. How to implement the promotion of chosen values? Particularly, who (State / Internet service providers / Content providers / Parents / Schools) is in charge of child protection?

Table 1: The different levels of considerations in Internet content regulation

Level 3: ethical considerations	Which values (protection of minors, respect for personal values, respect for cultural diversity, free speech,) to promote? In cases of value conflict, which one(s) should have priority? How to strike an appropriate balance between these contradictory values?
Level 2: social & political considerations	How to implement the promotion of chosen values? Who is responsible for child protection?
Level 1: financial & economic considerations	How to preserve the interests of the various providers involved?

The Concept of 'User-Empowerment'

"Central to the 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." (Centre for Democracy and Technology, 1999, p. 1) This clearly implies a choice at the socio-political level, as defined in the previous table: parents are considered solely responsible for child protection, thus they have to decide if they will filter Internet content or not and, if they opt to filter, they must then choose which kind of filtering they need.

Historically, the concept of 'parent empowerment' linked to Internet governance appeared in the US in 1995 as an Internet software industry reaction to the threat of government censorship. In June 1995, an association called the 'Information Highway Parental Empowerment Group' (IHPEG), was created by three leading Internet software companies (Microsoft Corporation, Netscape Communications and Progressive Networks) to focus on implementing a system that would enable parents to control the material on the net that could be accessed by their children (23). In August 1995, IHPEG was incorporated into the World Wide Web Consortium (W3C) (24).

Nevertheless, on February 8 1996, Senators Exxon and Coats' Communications Decency Act (CDA), was signed by President Clinton. CDA "made it illegal knowingly to provide indecent or manifestly shocking material to minors via electronic computer networks" (25).

The industry reacted in two ways:
-first, a coalition of publishers, content providers, access providers and civil liberties associations, attacked the legislation, claiming it invalidated the First Amendment (freedom of expression),
-then it stepped up its efforts to find an alternative [technical] solution to legislation... (26).

On June 26 1997, the US Supreme Court finally declared some of the provisions of the Decency Act unconstitutional. The reasoning held by the Court is based on the finding that the provision allowing for criminal

(23) http://censorware.org/pics/history/9506_ihpeg_birth.txt (Web site visited July 2000 but now deleted).
(24) http://censorware.org/pics/history/ (Web site visited July 2000 but now deleted).
(25) As regards the content of the Decency Act and its main provisions, see *inter alia*, Cannon, Nov. 96.
(26) Com(96) 483 Annexe IV p. 3.

sanctions for ISPs which have disseminated or helped to disseminate illegal or harmful content, was too vague and disproportionate. Indeed these criminal sanctions would create a risk that Internet providers would unduly restrict freedom of expression. The reasoning held by the Court also takes into account the specificity of Internet as a medium (27). Finally, the Court decided that there were other means of control that were less restrictive with respect to freedom of expression (28).

The US Report on controlling crime on the Internet (issued by the President's Working Group on Unlawful Conduct on the Internet on March 2000) continues to highlight the role of public empowerment which is "to prevent or minimise the risks from unlawful conduct involving use of the Internet." Moreover, on 23 October 2000, the US Commission of the Online Child Protection claimed (notably p. 9 and 10) that consumer empowerment (p. 41-44) has to be combined with public education, law enforcement and industry action in a co-ordinate effort of protection from online material that is harmful to minors.

The European Union has fully endorsed the approach of 'empowering parents to protect minors' (29), since the end of 1996. In September 2000, R. Swetenham of the European Commission (Bertelsmann Foundation, 2000) developed this concept, outlining the three pillars of Internet Content Regulation:

"Freedom of choice, control and information: Freedom of choice for the user to determine himself which Internet content he or his children can use. Control over access to Internet data that should be vested in the user rather than in any government. And finally information to support the user in making responsible use of the Internet."

In practical terms, user-empowerment in the domain of Internet content regulation comprises several components.

On the one hand, it includes the right of the Internet user to dispose of technologies in order to fulfil the need for protection. These technologies have to respond to several requirements (see below). They have to be adaptable so as to take into account respect for personal and cultural values.

(27) Two main characteristics define the originality of Internet as a medium vis-à-vis the press or audiovisual media: the first is the *non scarcity* of the medium and the second, the more "active" role of the consumer.
(28) *Reno vs. ACLU, 117 S.Ct 2329, 65 USLW 4715.* About this decision and its reasoning, see CUSTOS, 1998.
(29) See Com(96) 487 final, p. 19.

They must be transparent, i.e. make the user aware of any relevant information. They must also be diverse (i.e. providing technical variety), efficient and affordable.

On the other hand, user-empowerment includes the right to be informed of and educated on the risks linked to both the Internet and the available Internet filtering and labelling tools, to have efficient mechanisms to report any infringement and to have rapid, proportionate and adequate sanctions.

It is worth noting that the user-empowerment concept, which is advocated by the industry, many civil liberties groups and governments, now seems to be taken for granted. But we cannot help asking the following questions:

-Is it not the role of the State to protect children?
-Is it legitimate to charge parents with such a task?

Thus it is interesting to assess the opinions of the parents themselves in this domain:

- Are they worried when their children use the Internet?
- Which kind of solution do they suggest for protecting their children?

Several surveys are now available to some or partial answers to these questions.

In their sample of 1,001 American parents with at least one child (between the ages 8 and 17) and with (at least) one home computer connected to the Internet, TUROW & NIR (2000, p. 13) found that "about seven in 10 parents (71%) in 2000 agree with the statement 'I am concerned that my children might view sexually explicit images on the Internet" On the other hand, a poll (LAUNET, 2000) (by Ipsos *Libération* and Powownet) in France, has also shown that 62% of the (952) parents, which were interviewed in October 2000, are worried about the Internet use by their children: French parents (77%) fear pornography above all. According to the same poll, 54% of the parents agree that they themselves have to be primarily responsible for the web access control of their children while 20% think that the State should be chiefly responsible for this protective role, and 20% estimate that this responsibility must be first endorsed by ISPs. The final 5% believe that the content provider (30) should be primarily responsible for preventing child access to some web sites.

(30) Several techniques (such as for verifying age), suggested by the US Commission on Child Online Protection (2000, pp. 45-46), can be used by content providers.

Finally, it is worth noting that, according to the conclusion drawn by Morawski [31] from a Ipsos-Reid' survey, when compared to US parents, "European parents seem to have a much more relaxed attitude when it comes to what and how their children see and surf online."

■ A Means of Empowering Users: Filtering and Rating Techniques

The filtering techniques are "a means of empowering users by allowing their children to have access to a broad range of content on the Internet while avoiding contact with material that the parent would consider harmful" [32].

Keeping in mind the required qualities of the filtering services, we will first outline the technical framework of these services, then note the results of a survey we carried out on Internet filtering criteria and, finally, discuss some suggestions made by the Bertelsmann Foundation.

Technical framework

The filtering techniques currently available on the market are numerous (more than 100) [33], varied and complex. Comparisons are difficult (see, for example, CRANOR, RESNICK, & GALLO, 1998, or RYAN & TRIVERIO, 1999) each service has its own features. One issue is vagueness: on the one hand, the vocabulary is not universally accepted and frequently not (well) defined and, on the other hand, the technical framework is often not precise.

The following is an outline of the general framework (see also d'UDEKEM-GEVERS, 1999).

The 'filtering services' are considered *sensu lato*: they include any technical tool available for the end user which is involved in the process of Internet filtering, wherever it is located (PC filtering software packages, server based solutions,) and whatever it performs (providing only a rating criteria definition, providing a rating criteria definition and a rating, both classifying and filtering, filtering on the basis of ratings, etc.)

(31) See Ipsos-Reid, November 20, 2000.
(32) See European Union, Internet Action Plan (IAP), IST 2000 conference in Nice, France (6 8 November).
(33) See, for example, GetNetWise or The Internet Filter Software Chart.

The scope of Internet control (see table 2) can include topics or time. From a technical point of view, the topic control (or 'filtering') can be maintained either at the entry point level or at the content level itself.

At the entry point level, filtering of URLs (Uniform Resource Locator) can be based either on ratings (i.e. labelling) [34] only or on classifications into URL lists (generally 'black' lists (i.e. 'not for kids' lists/'NOT' Lists or, sometimes, lists of suggested sites) or on both ratings and URL lists.

One should note that rating and classifying are conceptually equivalent. Both imply that criteria (for classifying/rating) (e.g. word lists) have been defined beforehand. Both (see table 3) can be carried out either by human reviewers or by software or by human reviewers with the help of software.

PICS ratings are the most common. PICS stands for 'Platform for Internet Content Selection'. They constitute a set of technical standards which have been under development since the summer of 1995 by the World Wide Web Consortium (W3C) [35].

Let us point out that PICS allows the users to choose their label sources independently of their filtering software. The labelling of a site can be done by third parties (third party rating) [36] or by the content provider itself ('self rating'). Currently only web sites have received PICS labels. But "PICS labels can describe anything that can be named with a URL. That includes FTP and Gopher. E-mail messages do not normally have URLs, but messages from discussion lists that are archived on the Web do have URLs and can thus be labelled... Usenet newsgroups (OVERELL, 1996), and even individual messages, have URLs, and hence can be labelled. There is not

(34) The central concept and word 'labelling' is considered here to be synonymous with 'rating'. We would also like to emphasise that both these words are used in our text, but with two different meanings. On the one hand, we speak about the (electronic) labelling (or rating) of *Internet content* which can be used *by a technical filter* to control the access to this content and are usually not made to be seen by people. On the other hand, we also mention (visual) labels i.e. logos used as quality certification to be read *by people* to evaluate a *service or a product*. Of course, visual logos can certify that content has been electronically rated to be technically filtered.
(35) W3C was founded in 1994 to develop common protocols to enhance the interoperability and govern the web's evolution. It is an international industry consortium, jointly hosted by the MIT's (Massachusetts Institute of Technology) (US), INRIA (Institut National de Recherche en Informatique et en Automatique) (Europe) and the Kelo University Shonan Fujisawa Campus (Japan). Initially, the W3C was established in collaboration with CERN, where the Web originated, with support from DARPA and the European Commission.
(36) Surprisingly, the Mathonet et al. study (1999) which is entitled 'Review of European Third-party filtering and rating software and services' is however not limited to third party (filtering and) ratings as defined here but also includes what we call here 'filtering on the basis of black lists of URLs'.

yet an official URL scheme for IRC, but the PICS specifications defined a preliminary scheme, and a more robust URL scheme for IRC is being worked on" (37).

Filtering at the content level implies that both rating/classifying and filtering are managed in real time by software. It can be based on lists of words (i.e. in fact on criteria themselves). Currently, image recognition by software is in its infancy, cf. for example, Image Filter (KONRAD, 2000) by the firm LookThatUp.

The choice of a specific technique has practical results for the final user. The quality of three main filtering technique features must be assessed (see table 3):

-'reliability', defined as the capacity to take into account the context of a given content,

-'scalability', i.e. the capacity to manage the increasing number of web sites and

-'technical adaptability' which is considered in this paper as the capacity to handle the evolution and the possible changes of a given web site.

Control at the entry point level with rating/classification by human reviewers is the most reliable, although the least scalable and technically adaptable. Fully automatic control in real time has the lowest reliability and the highest scalability and technical adaptability. At present, it is unclear which system will eventually dominate.

As pointed out by the Commission on Child Online Protection, (2000, pp. 42-43), "No particular technology or method provides a perfect solution, but when used in conjunction with education, acceptable use policies and adult supervision, many technologies can provide improved safety from inadvertent access from harmful to minors materials."

Some filtering services are dedicated to a specific control (for example, time control or e-mail filtering). But frequently, an off-the-shelf filtering service provides several technical solutions for example, time control and topic control; control of topic at the entry point level and also at the content level; etc. Moreover, some services also include the control of outgoing information or of on-line applications (see table 2). The current market offer is very diverse.

(37) See W3C, PICS Frequently Asked Questions.

Table 2: Control scopes and corresponding possible technical solutions

Control general scopes	**Control specific scopes**	**Possible current technique solutions**
1.Topic control at the **entry point** (to an address or a file) level **(2 steps)**	1.1. Anything with a URL i.e.: - **WWW** (HTML Protocol) - FTP (File transfer Protocol) - GOPHER (for information research) - Usenet **News groups** and individual messages (NNTP Protocol) - TELNET (for terminal access) - [IRC Internet Relay Chat](N.B. e-mail messages do not have URLs) 1.2. (Local or on-line applications e.g. games, personal financial managers, etc.)	PICS labelling (self-rating or third party rating) and filtering Filtering on the basis of black/white **lists of:** - **URLs** or - Names of newsgroups, chat etc. Filtering on the basis of lists of application names/addresses
1. Topic Control at the **content** level itself **(1 step : real time)**	2.1. Incoming information 2.1.1. Anything with a URL 2.1.2. (Without a URL)N.B. for example, via e-mail (including their attachments) 2.2. Outgoing information (for ex. personal information via IRC, Web site questionnaire, e-mail, etc. or offensive words in search of sexually explicit sites or conversations)	**Lists of words (= criteria!)** + - Key word/string filter (or word-matching) / - Artificial intelligence based software
3. **Time** control	3.1. Hours/day 3.2. Days/week 3.3. Total by week	

Table 3: Technical solutions and their consequences

Control scopes	**Technical solutions**		**Consequences**
Topic **control**	Control at the entry point level 2 steps rating/classifying :	· By human reviewers · By human reviewers with the help of software. . By software only (web crawler,...)	***Highest 'reliability'*** Low 'scalability' Low 'adaptability'
	Control at the level of the content itself 1 step	Fully automatic in real time	Low 'reliability' ***Highest 'scalability'*** ***Highest 'adaptability'***

Summary of our survey on Internet filtering criteria

In this section, we will look at the results of a survey (UDEKEM-GEVERS, 1999) carried out by one of the authors of this paper in 1998 and early 1999.

Introduction

This survey analyses a large sample of current off-the-shelf filtering services to be used in the home or in the school, and even in companies. It focuses mainly on 'topic' filtering services (see table 2) and, particularly, on the access control to Internet sites (38) - i.e. anything with a URL (Uniform Resource Locator).

As a rule, the filtering services' providers base the process on documentation (sometimes including a 'demo' put on the WWW). Occasionally, this documentation is completed by analysing the downloaded filtering software itself or by e-mail correspondence with the provider. Filtering services totally devoted to businesses or with insufficient documentation are not considered.

The survey covers a sample of 44 filtering services. 9 are PICS rating services. Among the 35 other services, 31 are partially or totally based on URL/word/(other) YES/NOT lists and, among these 31, 22 are partially or totally based on NOT lists. From a technical point of view, the market provides a great deal of diversity.

Among the roles included in any Internet (URLs) filtering process as defined by RESNICK (1998), three are linked to filtering criteria: to define the criteria (39), to use them to rate/classify and to customise (or select) them.

Filtering services with a list to block

In the studied sample of 22 filtering services with a list to block access to web sites, classification criteria (see table 4) were mostly (20/22) fixed by the commercial firm which provides the filtering service. With the exception of two Canadian corporations, all these firms (i.e. 18) are located in US, many in California (5/20). Languages other than English were rare.

(38) Chat and e-mail are not considered here but are well known to be potentially dangerous for children (see for example LAUNET, 2000). "Recent research from the United States appears to suggest that nearly one in five young Internet users has been the victim of a sexual approach or solicitation online." (Internet Crime Forum IRC sub-group, October 2000).
(39) The criteria used for rating are the same used later for filtering.

On the other hand, 16 of the 17 filtering services mainly based on URL NOT Lists are themselves (either directly via the staff or indirectly via a software) responsible for classification of the web sites, on the basis of the defined criteria. In the sample of three filtering services working in real-time with artificial intelligence, the classification/rating is, by definition fully automatic, i.e. performed by a software written by the firm.

Table 4: Summary of those who defined the filtering criteria (in 22 filtering services with a list to block access - not linked to PICS)

Identification of the people/body responsible for definitions	Number	Location
Commercial firm	20 (but 2 with social concerns)	- 18: USA (5: California) - 2:Canada
Non-profit organisation	1	USA
Parent (implicitly)	1	

At this stage, customisation here can occur at two levels: classification criteria definition or URL. In the sample of 17 filtering services mainly based on URL NOT Lists:

-one gives full control to the final user without any predefinition,
-one provides the possibility of both adding to [or deleting] predefined criteria and of adding [or deleting] a URL (very high level of customisation),
-six provide a choice of predefined criteria plus the possibility to add (or delete) an URL (high level of customisation),
-six provide a choice of predefined criteria (only),
-only two provide fully customisable and visible Notlists,
-one provides only the possibility of adding/deleting a URL to/from the NOT lists,
-one does not provide any possibility of customisation.

In the sample of three filtering services working in real-time with artificial intelligence:

-three allow the list of words to be modified,
-one provides the possibility of adding a URL to a NOT List.

We can conclude that the analysed filtering services based on NOT lists provide the possibility of customisation (and sometimes of extensive customisation) but this customisation can only be brought into play in

categories predefined by the firm and in lists made by the firm. Let us add that the URL lists are, for the most part, undisclosed.

PICS ratings

As shown in table 5, those who set the criteria definition in the sample of PICS rating services analysed in 1998-99 were nearly all located in North America. All but one set of criteria was defined in English.

Table 5: Summary of those who defined the filtering criteria (in the sample of 9 PICS rating services)

Identification of the people/body responsible for definition	Number	Location
Commercial firm	4	- 2 USA - 2 Canada
Non-profit organisation	4	- 3 USA - 1 Italy
Private individual	1	- UK

On the other hand, among the 3 third party ratings, one rates via artificial intelligence and the other two do not carry out the labelling themselves but rely on outsourcing (see table 6).

Table 6: Synthesis of those who classify (in the sample of 9 PICS rating services)

Identification of the people/body responsible for classification	Number	Method
Self rating	6	N/A
Third party PICS rating services	3	- 1 (currently non-profit) : mainly artificial intelligence - 2: do not carry out the labelling themselves, but rely on outsourcing.

With PICS, the customisation/definition of filtering criteria can currently occur at 3 levels:

-choice of the rating source(s) (one or several),
-choice of the criteria available in the rating source(s),
-choice of the criteria levels (if any).

In future, it may be possible to use profiles (i.e. predefined filtering custom settings).

Ethical viewpoint

To 'fix criteria for rating/classifying' is not value-neutral and to 'rate/classify' can imply moral judgements. From an ethical point of view, it is thus very important that the final user (parent, teacher,) be able either do it him/herself (although this could be a considerable task) or find both criteria and a rating/classification in accordance with his/her own value judgements [40]. This last choice would be easier to implement using PICS since this standard allows the users to select their filtering software and their label sources independently.

In the sample we analysed, the observations made are ethically worrying.

First, with the exception of PICS, moral issues are central: the user is linked to the value judgements of the firm providing the filtering service, including the classification criteria and the classification itself into usually hidden lists. These hidden lists are considered by firms as part of their expertise, but they do not fulfil the techniques' transparency requirements. Firms claim to give control to the parents (or teachers), whereas it is firms themselves that have the control. Moreover, the available categories for filtering reflect mainly US values. Naturally, European users will not find that they suit their own cultural diversity. As regards customisation, it could require time and a certain level of expertise.

In PICS ratings, the situation is a little less negative than in other filtering services in the sample. The majority of criteria definitions are set outside the framework of firms and nearly half outside US However, all but one is in English! Moreover, these PICS services are still rare, and few filtering software applications can use them. The possibility, offered by PICS, of providing cultural diversity and independence from firms from the value judgement viewpoint, has not (yet?) [41] been fully exploited. On the other hand, with PICS, the customisation ('profiling') [42] could be carried out, in the future, by a third party chosen by the parents, and these would then only have to select the required age according to each of their children.

(40) The needed relevance of a filtering system to the different cultural background of member states is also stressed by KERR (2000, pp. 3 & 37-38).
(41) See KERR, 2000, pp. 4 & 5: "Self-labelling and filtering systems have the technical and theoretical potential to meet the needs of European consumers [...] The establishment of a viable system(s) is dependent on more content being labelled and/or on a workable combination of self-labelling and third party rating."
(42) A profile is called a 'template' in the Memorandum. See KERR (2000) for more on the profiles for future use.

Overall, we found that no off-the-shelf filtering service is currently adapted to European user cultural diversity. On the other hand, an attitude of *'laissez-faire'* towards the market seems not to be the best solution.

However, the situation which has been summarised in previous paragraphs is now improving, thanks notably to the multi-annual Community Internet Action Plan (IAP) (43) ("on promoting safer use of the Internet by combating illegal and harmful content on global networks"). The IAP was adopted in January 1999 and currently funds several projects, for example, 3W3S (44) or ICRAsafe ("Completing the system design to meet the requirements of European users") (45). This last project corresponds perfectly to some suggestions put forward by the Bertelsmann Foundation (see next paragraph).

Bertelsmann Foundation memorandum proposal analysis

At the 'Internet Content Summit' (46) of 1999, the Bertelsmann Foundation (47) presented its famous memorandum entitled "Self-Regulation of Internet Content". This text, fully endorsing the concept of user-empowerment (48), contains key recommendations for the Internet industry, policy makers, law enforcement authorities and users. These recommendations are allegedly based on reports by leading experts (49) from four universities around the world, and on the Internet User Survey that was carried out in Australia, Germany and the United States.

(43) See http://europa.eu.int/ISPO/iap/
(44) See http://europa.eu.int/ISPO/iap/projects/3w3s.html
(45) See http://www.europa.eu.int/ISPO/iap/projects/icrasafe.html
(46) See http://www.stiftung.bertelsmann.de/internetcontent/english/frameset.htm?content/c2200.htm. This summit was organised in Munich on September 9-11 1999 and funded by the Bertelsmann Foundation in co-operation with INCORE (Internet Content Rating for Europe).
(47) According to its own terms, "under private law the Bertelsmann Foundation is an independent foundation, its headquarters situated in Gütersloh (Germany). It pursues exclusively and directly non-profit making aims eligible for tax relief as defined in the Fiscal Code... In order to continue to be a creative force and to preserve its effectiveness and economic efficiency, the Foundation presently focuses its efforts in the areas of the economy, government and administration, media, politics, public libraries, medicine and health services, cultural activities, foundations and higher education".
(See http://www.stiftung.bertelsmann.de/english/ueberbl/grundl/index.html.)
One should note that this foundation was started by the eponymous media giant, which is also AOL's partner in Europe.
(48) It considers (p. 10) self-rating and filtering systems as "empowering user choice".
(49) In fact, the experts have hardly criticised the fact that the final Memorandum were considered representing the faithful outputs of their reports.

In October 1999, the US Centre for Democracy and Technology (CDT) (50) published a response online (51) entitled "An Analysis of the Bertelsmann Foundation memorandum on Self-Regulation of Internet Content: Concerns from a User-empowerment Perspective". In this paper, CDT condemned the Bertelsmann Foundation memorandum in the name of 'free speech'.

We will now look at some of the suggestions made by the Bertelsmann Foundation. Some of these suggestions are worth analysing for two reasons. First they help clarify our discussion on filtering techniques as a means of empowering. Second, discussions within the context of CDT allows conflicting interests to be put forward and debated.

One suggestion made by the Bertelsmann Foundation (p. 56) entails the "development of an international self-rating/filtering system".

It must be pointed out that, from the point of view of an adapted and effective control by parents, the solution suggested by the Bertelsmann Foundation has several advantages (see table 7).

- First, it plans to entrust the responsibility for defining the selection criteria (i.e. "the initial basic vocabulary", according to the terms of the memorandum) to a non-profit and independent organisation, "not under the auspices or control of any particular business organisation" (see the Bertelsmann Foundation text p. 35). This point favours respect for personal and cultural values and is worth underlining. Indeed defining the criteria is a crucial role. It automatically influences subsequent steps of the filtering process (assigning labels and selecting filtering criteria) but, as pointed out by CPSR (1998) (52), "in general, the use of a filtering product involves an implicit acceptance of the criteria used to generate the ratings involved [...]

(50) As explained on its home page (See http://www.cdt.org/mission/principles.html.), the Center for Democracy and Technology (CDT), located in Washington DC, is "a non-profit public policy organisation dedicated to promoting the democratic potential of today's open, decentralised, global Internet". Its mission "is to conceptualise, develop, and implement public policies to preserve and enhance *free expression*, privacy, open access, and other democratic values in the new and increasingly integrated communications medium. CDT pursues its mission through research and public policy development in a consensus-building process based on convening and operating broad-based working groups composed of public interest and commercial representatives of divergent views to explore solutions to critical policy issues. In addition, CDT promotes its own policy positions in the United States and globally through public policy advocacy, online grassroots organising with the Internet user community and public education campaigns, and litigation, as well as through the development of technology standards and online information resources".
(51) See http://www.cdt.org/speech/991021bertelsmannmemo.shtml
(52) SR stands for Computer Professionals for Social Responsibility. It is a US 'public-interest alliance of computer scientists and others concerned about the impact of computer technology on society'.

Parents should take care to insure that the values behind the ratings are compatible with their beliefs." Will it be possible, however, to establish enough criteria and to include sufficient nuances to reflect all the different European cultures?

- Second, the Bertelsmann Foundation solution entrusts to third parties the selection of criteria (i.e. "the production of templates", in the words of the Bertelsmann Foundation) "that match their particular set of values and beliefs". It aids parents in their task: they will have only to choose a relevant template (KERR, 2000, p. 6). This point thus further promotes respect for personal and cultural values and contributes to the efficiency of the technique.

- Third, the suggested solution of "a single comprehensive rating system" is interesting from a conceptual standpoint: the more extended a standard is, the more useful it is for the users. A frequently used vocabulary standard should provide benefits both at the level of rating and the level of criteria selection, and thus provide greater efficiency. The challenge with this solution will be to define a vocabulary with enough nuances to allow reflection of the different cultures.

- Fourth, the Bertelsmann Foundation recommends incentives for self rating (however, its text on this topic (53) is ambiguous in terms of the governments' role). This recommendation furthers the dissemination of the ratings in order to reach a critical mass, and to achieve efficient rating and filtering techniques.

These last two points in particular have been criticised by CDT. Indeed, according to CDT: "This [global co-operative filtering system suggested by the Bertelsmann memorandum] raises the spectre of mandatory labelling, for without mandatory labelling, a substantial portion of the content will likely remain unlabeled. But mandatory labelling is a form of forced speech, and therefore an infringement on the freedom of expression." One should note that, contrary to the concern put forward in its paper title, CDT is defending content providers' right to free speech, but not parents' empowerment (see table 7). The Interests of parents and of the media (or content providers) are conflicting. From a final user-empowerment perspective, creation (by governments or by content providers) of incentives for rating or even mandatory labelling could be perceived as a good initiative! The more sites

(53) Bertelsmann Foundation 1999, p. 34 : "Governments can encourage the creation of filters through, for example, tax incentives. However governements should not impose criminal sanctions for failure to rate web sites... Content providers worlwide should be mobilized to self-rate..."

labelled with a standard, the more efficient any filtering services based on that standard.

The technical solution suggested by the Bertelsmann Foundation also has several drawbacks, however. As pointed out by CDT, the issue of the unlabelled sites (54) remains unsolved. Moreover, it is not a fully satisfactory solution (it has to be completed, if the parents wish, by other tools for example to control ingoing e-mail or outgoing information or to set time limits on children's access).

Table 7: Filtering and rating techniques: in the Bertelsmann Foundation text and its review by the US Centre for Democracy & Technology (CDT)

User (= *parent*) empowerment to control content		*Content provider* free speech
1. *Respect for personal and cultural values* → rating/filtering vocabulary(/ies) defined by independent non-profit organisation(s) (as suggested by the Bertelsmann Foundation) → possibility of customisation by various independent non-profit organisations (cf. for example 'templates' as suggested by the Bertelsmann Foundation)		
2. *Technical diversity* (as advocated by CDT)		
3. *Efficiency* of the various filtering techniques: (notably) thanks to maximisation of the number of labelled sites → creation of incentives for rating (as suggested by the Bertelsmann Foundation) (55) → a single rating vocabulary (as suggested by the Bertelsmann Foundation)	↔	*No compulsory labelling* (as advocated by CDT)

Another drawback, although not criticised by CDT, lies in self-rating: this solution (56), provides a higher risk of subjective labelling (or even of mislabelling) (KERR, 2000, pp. 39-40). Nevertheless, a system of liability in the case of false or deceptive statements (57) is still possible whenever self-

(54) According the KERR's analysis (2000, p. 3) the problem of unrated sites is the 'main problem' of the current state of filtering and rating techniques.
(55) It is worth pointing out that the US Commission on Child Online Protection (2000) recommends incentives for ratings by content providers.
(56) Nevertheless, self rating has also been recommended by the Action Plan approved by the 'First World Summit for Regulators' (30 November - 1 December, Paris, UNESCO).
(57) This is the system available in US under the False and Deceptive Statement Act, which grants the right to provide an injunction in case of false or deceptive statement to the Federal Trade Commission (FTC).

rating is incorrect. In any case, for more objective judgements, third party rating is a better (but sometimes more expensive) solution. Nonetheless, the third-party rating solution is not a panacea: it could require additional protection for their users: it would be adequate to ensure, through appropriate information on their web sites, transparency in terms of the persons or associations which are behind the work done and to enforce a system of liability in case of negligent behaviour in the rating of the web sites. Such individuals are still rare (see table 6) but, in the future, it seems that they would often be non-profit organisations and would consider this last requirement as impracticable. Third party rating should take place in combination with self-rating (58). Finally, the proliferation of rating systems could create confusion among web users.

On the other hand, CDT considers technical diversity provided by the market as the basis of parent empowerment. We admit that this diversity contributes to parents' empowerment in so far as it does not result in parents' confusion. However, it is our view that, from a final user standpoint, respect for values is probably more important and should not be neglected on the pretext of free speech, particularly in European countries (59).

In agreement with Grainger, the representative of the Australian Broadcasting authority (ABA) (1999, pp. 53-54), we believe that:

"It is essential for policy makers and legislators, as they [...] prepare new rules for [...] the Internet, to revisit and restate the public interest objectives they believe should apply to those industries and their governance. Sweeping references to the 'public interest' may be less effective than a clear articulation of the process concerns that legislators are seeking to advance [...]" (60).

With regards to the Internet, free speech (as so frequently underlined in US), the protection of minors, respect for personal values and respect for cultural diversity are among the public interest objects to be achieved.

(58) This is also one of KERR's conclusion (2000, p. 43).
(59) GRAINGER' analysis (1999, pp. 53-54) states :"Whereas in the United States of US Constitution First Amendment allows the free speech lobby to dominate discussion about self-regulation, other countries with healthy democratic systems and vibrant process of open expression are able to seek a more appropriate balance between the right to free expression and the right of communities to nurture national and local cultures and to protect children from harmful content..."
(60) Compare with our assertion: "We should like to stress the State's vital obligation to intervene at a time when in our opinion deserting the Internet and withdrawing from the field of regulation to such a point that it no longer even decides the general framework, would notably put at a risk public order, fundamental liberties and other basic values." (POULLET, Oct. 2000).

■ User-Empowerment in the General Framework of Co-Regulation

Filtering services and user-empowerment must now be replaced in the global framework of Internet content regulation.

One should note that even if it does not use the word 'co-regulation', the Bertelsmann Foundation text fully promotes this mode of regulation.

But this coalition between private and public regulators is considered by CDT as a great danger for citizens' fundamental liberties such as the freedom of expression and right to privacy.

We believe that the joint regulation of the Internet is both necessary and promising. For this reason, we will now return to this paradigm.

Co-regulation is an ambiguous concept since it covers so many different mechanisms and areas. Thus our intention is now to try to better identify the possible roles of each partner and their possible co-operation in a process of co-regulation of the Internet.

We will set out a non-exhaustive list of tasks which could be involved in such a process. Among these tasks, some have been already included in an effective joint regulation, e.g. in Australia (61), some have been suggested or envisaged, e.g. by the Bertelsmann Foundation (1999) or in USA (62), while others are being put forward for the first time here.

We will take into account the possible players: private sector or public authorities (state or international organisation).

We will also propose that three levels of action be distinguished. The first level, the most important in terms of user-empowerment – and rightly praised by CDT – concerns the mechanisms put at the disposal of each individual for exercising his/her freedom. At this level, we will analyse, in particular, the problem of labelling and filtering mechanisms. The second level, emphasised by the Bertelsmann Foundation memorandum, is the collective answer given by the sector itself in order to provide solutions when the mechanisms of the first level are insufficient or inadequate. The third

(61) Since the Australian Broadcasting Services Act 1992 as amended is based on this approach, we will make extensive reference to the Australian solution. It is worth noting that the Australian texts use the term 'co-regulation' to refer to their new regulatory regime.
(62) Cf. Departments of Labor, Health and Human Services, and Education, and related Agencies, H.R.4577- Appropriations Act, 2001.

level concerns the final response to be given both by the legislator and the judges.

Thus, we will merely outline a grid of analysis for this new paradigm (see table 8). In this grid we will try to locate correlated tasks by different players (inside a level) on the same lines.

We do not consider this grid as the perfect solution to be implemented. Nevertheless, we will take advantage of this analysis to outline our opinion on some of the possible elements of co-regulation.

First level of action: filtering and labelling techniques

Concerning the first level, the development both of various filtering techniques and of labelling systems and activities is the best method of providing (in a totally decentralised manner) a solution that will take into account and respect the infinite diversity of opinions, cultures and sensitivities of the people throughout the world.

Role of the private sector

The private sector will play the first role in the development and financing of these products (63) and services. It is the role of the private sector to develop and finance, within a competitive environment, value-neutral software and products capable of supporting the rating and filtering activities (in particular, we may refer to new developments such as software that takes into account the context of a picture or text, or, software that provides the user with the possibility of adding specific details such as their own personal 'green/white' lists). The US Commission on Child Online Protection recommends, in particular, (2000 p. 42) that "industry take steps to improve child protection mechanisms, and make them more accessible online." It is the role of services providers, but also of churches, unions, parents' associations, private or public youth protection associations, schools, etc. to offer rating services (64) in employing the platforms developed by the software and filtering systems producers.

(63) These two tasks are envisaged e.g. by the Bertelsmann Memorandum, 1999 (p. 56).
(64) The system should have to support the development of profiles established by these associations considered as trusted third parties. The individuals must have the possibility of downloading these profiles (see above and table 7) according to their cultural, philosophical or ideological preferences.

The role of the private sector is also to achieve a good marketing of its services on a scale which makes the use of these products and services significant, in other words so that a critical mass of labelled Internet services might be obtained. There is also a clear need for promotion of labelling and filtering systems on a national or language group basis.

On the other hand, in the Australian example, several other obligations (65) are imposed on the Internet industry: first, there is the obligation to provide the users with filtering tools and information (66) about these tools and then, in the framework of the Internet Industry Codes of Practice (Internet Industry Association, 1999), to provide a mechanism of product/service approval (67) and also to encourage commercial content providers to use appropriate labelling systems. As for the US Commission on Child Online Protection (2000 p. 46), it claims that the adult industry "should pursue efforts to encourage web sites to self-label and should provide incentives (68) for them to do so."

Role of the public authorities

The diversity of rating services has to be supported, while the State's role is clearly to encourage the development of the filtering and labelling techniques, to promote their use by the citizens through appropriate educational programmes and to ensure a certain pluralism corresponding to the attempts of the different groups of citizens.

Furthermore, it is possible to project that public regulation will require these private initiatives to be transparent as regards the criteria used for the selection and even the 'black' lists to block (69), the methods followed and the persons in charge of the system (70). One could imagine that a public

(65) See Internet Industry Association, December 20 1999 - updated 2000 and Internet Industry Association, December 16 1999- updated 22 December. It is worth noting that, according to the Australian regulatory regime, "ISPs will not be required to evaluate the content themselves" and "are not required to ensure that end-users install or operate the filters".
(66) In this domain, the US Commission on Child Online Protection (2000, p. 41) recommends that "the private sector – industry, foundations and public interest organizations – provide support for an independent, non-governmental testing facility for child-protection technologies."
(67) A list of filters approved by the Internet Industry Association is included in the Internet Industry Codes of Practice. This list is not endorsed by ABA (see LEBIHAN, 2000).
(68) One should remember that according to the suggestions of the Bertelsmann Foundation, State should be responsible for the creation of incentives for rating.
(69) The US "Copyright Office said it should be legal for users to access such lists, in part so people can criticize and debate them." (WILDE, October 27, 2000).
(70) The Commission on Child Online Protection (COPA) Report to US Congress (Oct. 2000) estimates that "Resources should be allocated for the independent evaluation of child protection technologies and to provide reports to the public about the capabilities of these technologies".

mechanism of approval or certification (e.g. logos, ...) would be put at the disposal of the firms which voluntarily want to see certain fixed qualities of their system recognised. It also seems that certain measures must be taken to prevent mislabelling (71) since this practice may deeply affect users' confidence in the web, and cause them harm. Moreover, price control might be exercised by the State, particularly in the case of incorporating filtering techniques as a basic service of the browser without additional costs.

The State could also require ISPs to provide users with filtering tools and information about these tools. This obligation is already included in the new regulatory regime in Australia, as quoted above.

On the other hand, public organisations could make available relevant information to be included in lists. This has been suggested by the US Commission on Child Online Protection (2000, pp. 9 and 43-44 (72)). More concretely, the Bertelsmann Foundation (2000) announced that "Germany's BKA (federal criminal investigation department) will make a list of known Nazi sites available to the ICRA filter system in the form of a negative list."

Finally, the state would provide schools or other educational agencies with incentives to use filtering techniques. Note that a US Bill (73) regarding the purchase of computers used for Internet access is currently being introduced in order to forbid the provision of any funds to schools or other educational agencies "unless such agency or school has in place, on computers that are accessible to minors, and during use by such minors,

(71) Cases of mislabelling (and thus 'overblock') have already been condemned. See, for example, the famous 'breaking of Cyber Patrol' by JANSSON & SKALA (2000). See also BOWMAN (2000), LEBIHAN (2000) and FINKELSTEIN (2000). The Cyber patrol case is of interest. The publication of the list of blocked Web sites by people who had bypassed the weak security measures developed by Cyber Patrol had revealed that the Cyber patrol filter was blocking certain web sites for competition reasons and not for their illegal or harmful content.
Cyber patrol has sued the infringers for violations of the Digital Millenium Copyright Act of 1998 (see Act, infra) which grants protection for the persons who have installed technical protection measures in order to prevent copyrighted works. According to the arguments of Cyber patrol, the list of blocked web sites was copyrightable. In our opinion, this argument is not acceptable since the criteria used by the filtering operators must be transparent, and certain control may be exercised to ensure effective respect. It would be too easy to take the argument of copyright in order to prevent any access to the list of blocked web sites.
(72) "The Commission recommends that state and federal law enforcement make available a list, without images, of Usenet newsgroups, IP addresses, World Wide web sites and other Internet sources that have been found to contain child pornography or where convictions have been obtained involving obscene material. This information may be used to identify obscene materials or child pornography under the control of ISP or content provider."
(73) See Section 304 of the Departments of Labor, Health and Human Services, and education, and related Agencies, H.R.4577- Appropriations Act, 2001. See also excerpts of this Act made available by CDT at http://www.cdt.org/legislation/106th/speech/001218cipa.pdf_This act was passed by both the House and Senate on December 15 200 (see Center for Democracy and Technology, 18 December 2000).

technology which filters or blocks (1) material that is obscene; (2) child pornography; (3) material harmful to minors".

With regards to the question of interoperability of the different rating systems, it would have to be analysed and encouraged by international public organisations since it will provide each Internet user throughout the world with better knowledge of the meaning of the various criteria used by the multiple labelling services (74).

Comment

If, for reasons expressed above, this first level is the most important, it is quite obvious that the solutions provided are not sufficient. For example, it would be contrary to the right to freedom of expression to impose a label on each web site. It would be contrary to the data protection requirements to forbid the development of anonymous mail and web sites on the Net. Secondly, as previously stated, due to the permanent evolution of the content of each web service, the labelling services might not offer a perfectly secure system. That is why other levels of action must be considered.

Second level of action: first response to the insufficiencies of level 1

The second level is a response to level one's insufficiencies.

Role of the private sector

A collective answer is proposed through codes of conduct or practice (75), hotline (76) mechanisms, in addition to various private sanctions such blocking of infringing web sites, publication of black lists, etc. This answer might be offered individually by an IAP or an ISP or jointly by a consortium of different providers at regional, European or global level. This second level offers complementary solutions to the first level. So, if I discover racist

(74) KERR (2000, p. 44) draws a similar conclusion when he pleads for "an international standards body to co-ordinate the process of developing the systems and to monitor their interoperability, quality and security."
(75) The Commission on Child Online Protection (2000, p. 44) "urges the ISP industry to voluntarily undertake 'best practices' to protect minors."
(76) "facilities for easy reporting of problems to the parties who can address them, either online or via telephone. Such hotlines would bring problems to the attention of both relevant government authorities and private sector groups that can act in response to reported problems." (Commission on Child Online Protection, 2000, p. 32).

discussions in a forum, I can alert the IAP, an association of IAPs. or an ADR through a hot line mechanism, following which highly effective measures might be taken to stop this illegal action.

On the other hand, it is worth noting a recommendation made by the US Commission of the Online Child Protection (2000): "government and Industry should effectively promote acceptable use policies." (p. 41). Acceptable use policies mean : "Establishment by a parent or an institution (school or library) of rules regarding the types of materials that may be accessed. Typically, such policies would be enforced by means of denial of further access in the event of a violation." (p. 36).

The main fear relating to this second level of control is the over-censorship that it might create since the alerted IAP may be urged to act in order to avoid any problem with the "plaintiff," even if, ultimately, it is established that no illegal or harmful content exists. The risk of action on the basis of a *prima facie* infraction is high. That is why certain limits must be imposed on the self-regulatory solutions.

Role of the public sector

First, it must be clear that the possible sanctions must be taken only according to a certain procedure which does respect the basic principle of a fair process. Thus, the US Digital Millennium Copyright Act (DMCA) (77) has enacted the obligation for the IAP or other intermediary services to set up a procedure of "notice and take down notice" plus a "put-back procedure" (78). This procedure deals with complaints relating to copyright infringements but it would be usefully extended it to illegal or harmful content. First, it requires complaints to be accompanied by specific details and a signature and, second, it requires that the alleged violator be notified before any action is taken. Other requirements may be proposed: first, the transparency of the criteria and subsequent procedure must be ensured. The concrete implementation of the criteria and of the procedure must also be subject to possible control (79). Except for provisional decisions in cases of obvious

(77) See Senate and House of Representatives of the United States of America, 1998. According to the Sect. 512 (c) 1 a hosting service provider who expeditiously blocks access to material if he receives a notification of a rights holder claiming that the content concerned infringes his copyrights, he will avoid liability.
(78) According to the Sect.512 (c) and (g) of the US Digital Millenium Copyright Act, the person whose material has been removed has the right to object and to have his material put back on the net. See Julia-Barcelo, 2000.
(79) See the Cyber Patrol case (supra) where the filtering operator denies the right of a third party to access the list of blocked Web sites in order to verify its compliance with filtering criteria.

infringements (80), the setting up of Alternative Dispute Resolution Mechanisms respecting the main principles of a fair process (81) is needed before taking definitive sanctions or decisions. Secondly, Data Protection principles and competition must be fully respected when establishing and implementing the self-regulatory provisions and jurisdictional mechanisms.

On all these points, the Australian case may be cited. First, the Australian State has required the Internet Industry Association (IAA) to develop codes of practice. The 'IAA Internet Industry codes of Practice' were registered by the Australian Broadcasting Authority (ABA) on 16 December, 1999 (82). They aim mainly to facilitate end-user-empowerment.

We think that, via suitable legislation, the role of the State should be to promote and eventually to approve appropriate self-regulatory solutions. In so doing, the State will naturally have to remind the self-regulators of the limits of their scope of action. Moreover, Article 10 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms clearly asserts that any limits relating to freedom of expression must have legislative grounds, must be specified and limited to what is strictly needed to achieve the specific public interest objectives pursued and described by the legislation (83). If the private self-regulators may help the pursuit of these objectives, any eventual action they take must fall within these limits (84).

(80) In these cases, a notice must be sent immediately to the public authorities (see level 3).
(81) These principles, enacted by article 17 of the European Parliament and Council Directive on E-commerce (2000), are the following: impartiality and qualification of the "judges", accessibility and convenience for Internet users, transparency of the functioning and of outputs, adversarial procedure, possibility of representation.
(82) See also, the annex of the (E.U.) Council Recommendation of 24 September, 1998 (which fixes the minimal requirements of the codes of conduct concerning Internet content and the protection of minors) and the following COPA recommendations (2000) : "Government and industry should effectively promote acceptable use policies".
(83) This Article asserts: (1) "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without the interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring licensing of broadcasting, television or cinema enterprises ". (2) "The exercise of these freedoms, since it carries with it duties and responsibilities, may not be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic Society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for the prevention of disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."
Regarding art. 10 of the Council of Europe Convention and the similar provision included within the Universal Declaration of Human Rights (art.19), see Global Internet liberty Campaign (GILC), Sept.98. A summary of the case law of the European Court of Strasbourg may be found in Lester 1993.
(84) In our opinion, Article 10 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms is also applicable *vis-à-vis* private authorities when these private authorities illegitimately censor the content on the basis of an explicit or implicit delegation of powers by the public authorities.

On the other hand, as suggested by the Bertelsmann Foundation (1999), the State should co-operate with the national hotline. And as cited above, in co-operation with industry, it should promote acceptable use policies (cf. Commission of the Online Child Protection, 2000).

Moreover, national hotline co-operation should be encouraged by International organisations.

Third level of action: final answer to the insufficiencies or the 'latest word'

The third level is action taken by public authorities themselves, and possible co-operation with the private sector in this action. The privilege of the official jurisdictions is to have the last word. No self-regulatory solution may therefore hinder or restrict the right of a person or a body to go before a Court or an administrative body, either to judge the problem in the case of illegal or harmful content, or, according to the exequatur procedure, in the case of private arbitration, to verify whether the self-regulatory solution effectively respects the main principles of Society, i.e. public order. Here, a recent case (85) is rather pertinent: on 20 November, 2000, "a French court ruled that US-based Yahoo, Inc. is to be held liable under French law for allowing French citizens to access auction sites for World War II Nazi memorabilia. The court ruling on Monday subjects Yahoo to fines in excess of 100,000 francs (US$12,853) per day unless it installs a keyword-based blocking system that prevents French citizens from seeing the offending Yahoo sites." (Centre for Democracy and Technology (CDT), November 21, 2000).

After having determined the illegal nature of certain content through appropriate jurisdictional means, it is then the State's role to take any appropriate tools in order to prevent any access to this content and, in that context, to impose certain duties on the online intermediaries. It is worth noting the way in which these requirements have already been implemented in an example of co-regulation: "Internet Content Hosts in Australia must take down content that has been the subject of a complaint to the ABA, and the ABA deems the content to be in breach of Australian law [...] There are heavy penalties for ISPs for non-compliance." (Internet Industry Association, December 20 1999 - updated February 2000) This solution to bring the supposed infringing Internet service before the ABA does not exclude the possibility of going before another jurisdiction including a private ADR or another official

(85) See Tribunal de Grande Instance de Paris, *Ordonnance de référé du 20 novembre 2000.*

jurisdiction (86). The main objective of intervention by an official jurisdiction is, ultimately, to avoid any private censorship and to impose on all the Internet service providers the obligation to block any infringing content of which they are aware. Note also Yahoo! UK's decision "to employ a Yahoo! 'inspector' charged with ensuring that Yahoo! Messenger system is not polluted with paedophile content." (BARRY & MCAULLIFFE, 2000). Yahoo! UK also promised that, at the request of organisations such as Childnet International and the police, it may be willing to abolish chat-rooms because of the threat of paedophiles. Still more recently, Yahoo US said "that it would try more actively to keep hateful and violent material out of its auctions, classified sections and shopping areas." (GUERNSEY, 2001) Indeed it will use a software "that that automatically reviews information that sellers are trying to post on the Yahoo Web site. If the software detects something in the submission that appears to violate the company's standards, the seller will immediately receive a message with links to Yahoo's terms of service. The seller can then revise the listing or appeal to Yahoo's staff for human review" (GUERNSEY, 2001).

Table 8: Grid of analysis of Co-regulation: the different levels of action, some possible roles and corresponding players

Levels of action	Players and their roles		
	Private sector	Public authorities	
		State	international organisation
Level 3: Final answer to the insufficiencies		- (Court or administrative body:) either to judge the problem or to check if the self-regulatory solution effectively respects the main principles of Society.	
	- to co-operate with public authorities to fight illegal content (traffic records,...).	- to request private sector co-operation in the fight against illegal content.	- to encourage national policy co-operation
		- to deploy any appropriate tools in order to prevent any access to these content and,	
	- (ISPs:) to block any infringing content of which they are aware	- in that context, to impose certain duties on the on line intermediaries	

(86) It is not a given that an administrative authority, competent in the field of audio-visual services, is the most appropriate choice for solving issues linked with the protection of minors. Undoubtedly, the competence of traditional criminal courts acting urgently would be a better solution.

Level 2: First response to the insufficiencies of level 1	- to develop codes of conduct/practice - to promote acceptable use policies / family contract (87) - to be responsible for various sanctions - to create and finance (88) hotlines	- to promote (through legislation) and, eventually, to approve/register appropriate self-regulatory solutions (particularly: private sector codes of conduct/practice (89) - to promote acceptable use policies / family contract - to remind the self-regulators of the limits of their actions - to co-operate with national hotlines	- to encourage national hotline co-operation
Level 1: Filtering and labelling techniques	- to develop and finance the techniques - to provide the users with filtering tools and information about these tools - (in the framework of codes of conduct/practice) to provide a mechanism of product/service approval - to obtain good marketing of their services - (in the framework of codes of conduct/ practice) (90) - to encourage commercial content providers to use appropriate labelling systems	- to encourage the development of the labelling and filtering techniques - to require ISPs to provide the users with filtering tools and information about these tools - to provide a mechanism of filtering service approval - to promote the use of technology by the citizens (notably through an appropriate educational programmes) - to foresee certain measures against mislabelling - to ensure a certain pluralism - to require transparency from private initiatives - to control prices - to make available relevant information to be included in black (/white) lists and used either on a voluntary basis by people or by filtering services (91) - to provide schools or other educational agencies with incentives to use filtering techniques (92)	- to encourage rating system interoperability

(87) Cf. Commission on Child Online Protection, 2000.
(88) Cf. the Bertelsmann Memorandum (1999, p. 56).
(89) Cf. the Australian example.
(90) See also § 13 of the Hong Kong Internet Service Providers Association's Code of Practice - Practice Statement on Regulation of Obscene and Indecent Material.
(91) Cf. the Germany's BKA (federal criminal investigation department) example as mentioned in Bertelsmann, 2000.
(92) Cf. Departments of Labor, Health and Human Services, and Education, and related Agencies, H.R.4577- Appropriations Act, 2001.

Another possible initiative by public authorities would be to request the co-operation of the private sector in the fight against illegal content. As we have pointed above, many of the recent laws have made this co-operation mandatory and required that public telecommunication services providers (IAP, hosting providers, Certification Authorities and intermediary services like search engines) both keep systematic records on the different uses of their services and check the real identity of their subscribers. Much of this legislation does not respect the limitations imposed by the Council of Europe Draft Convention on Cyber-crime (2000) and its case law since they are trying to legitimize disproportionate means of processing personal data in view of public interest objectives. Some Acts (e.g. the Belgian one) require that the telecommunication service providers store the data on subscribers' use of the Internet for 12 months (e.g. the web sites and the pages visited, the time, the duration of the visit, the keywords entered into a search engines), and to allow the authorities access to this data even if there is no specific case against a particular person. We think that this kind of mandatory co-operation creates a high risk of a global network surveillance, and goes well beyond what would is acceptable from a data protection perspective.

National policy co-operation should be encouraged by international organisations.

■ Conclusions

The European Union's official texts relating to illegal and harmful content regulation on the Internet have evolved. They began (prior to '98) by supporting private sector leadership, then (98-99) began to encourage private – public co-operation and, finally (since 2000), they have been giving the State an increasing amount of investigative power, while at the same time limiting Internet players' liability.

These European texts clearly diverge from the corresponding US ones in terms of the importance given to the respect for cultural diversity.

The concept of 'parent empowerment' linked to Internet content governance appeared in US from 1995 as a reaction by the Internet industry to the threat of the public censorship. It is indeed the leitmotif of the libertarian associations and of advocates of 'free speech' which are so powerful in US. It implies that parents – not the State – are deemed to be in

charge of child protection on the Internet. This concept has been quickly and definitively adopted, first by the US government and then by the European Union.

The corollary of the concept of 'user-empowerment' is the use of Internet filtering techniques by parents. Concerning these techniques, we suggest a framework to help promote better understanding, and wish to stress the importance of labelling techniques (notably with PICS) as an effective means of empowering parents. We refer again to the conclusions of our survey on 44 off-the-shelf filtering services from the filtering criteria viewpoint (93). This survey showed that the market alone is unable to answer the need for a variety of European user opinions and cultures. And, contrary to the view of some free speech US lobbies, we would like to stress that 'user-empowerment' also carries the basic implication that all users can make value judgements particularly without having to refer to the judgements of American firms and industry.

'User-empowerment' is a conceptual element which can be included (or not (94)) in the self-regulatory and co-regulatory paradigms (but not in the purely public regulation one). It includes the right of the Internet user to be informed and educated about the risks linked to both the Internet and the available Internet filtering and labelling tools. It also involves the user's right to dispose of efficient, diverse, transparent, affordable and adapted technologies and services to respond to their need for protection. On the other hand, it involves the user's right to have efficient mechanisms to report any infringement and, in these cases, to have rapid, proportionate and adequate sanctions. To ensure these rights, public authorities must intervene. But the private sector alone is in charge of providing competitive, flexible and scalable solutions which manage the cultural, philosophical and ideological diversity. The role of public authorities is both ancillary and essential vis-à-vis the private sector. Ancillary, because a public authority's intervention might never be a substitute for private intervention, while it must promote this intervention (95) as a way of ensuring the Internet user's rights.

(93) Three main questions have been asked: Who is responsible for defining the filtering criteria? Who uses them to classify or rate web sites? How can they be customised?
(94) In this case, the private sector should be in charge of the protection of minors.
(95) See the 1998 UN Report of the Special Rapporteur, Mr. Abid Hussain (last § of C. The impact of new information technologies): "The Special Rapporteur is of the opinion that the new technologies and, in particular, the Internet are inherently democratic, provide the public and the individual access to information sources and enable all to participate actively in the communication process. The Special Rapporteur also believes that action by States to impose excessive regulations on the use of these technologies and, again, particularly the Internet, on the grounds that control, regulation and denial of access (necessary to preserve the moral fabric and cultural identity of societies) is paternalistic. These regulations presume to protect people from themselves and, as such, they are inherently incompatible with the principles of the worth and dignity of each individual. These arguments deny the fundamental wisdom of individuals and societies and ignore the capacity and resilience of citizens, whether on a national, State, municipal community or even neighbourhood level, often to take self-correcting measures to re-establish equilibrium without excessive interference or regulation by the State."
(96) Althoug the Commission on Child Online Protection recommendations do not use the word co-regulation, they are clearly in favour of this regulation paradigm.

Essential, because the State's main role, bearing in mind the limits imposed by fundamental human rights (privacy and freedom of expression): to assert the Internet user's rights to be protected against illegal and harmful content by creating an appropriate regulatory framework (which includes promoting self-regulatory measures). In that sense, we plead strongly in favour of a co-regulatory approach. It would comprise three levels of action: the first composed of filtering and labelling techniques, the second is an initial response to the insufficiencies of level one and the third is the final solution. At each level, there are various possible roles to be attributed to the private sector or the public authorities in order to make them collaborate. There are several possible means of implementing the paradigm. We think that this joint regulation of Internet content is necessary and promising but must be kept within limits to avoid the risk of a global surveillance of the networks.

As the US Commission on Child Online Protection concluded in its report to the Congress (October 2000, p. 9) (96): "After consideration of the information gathered through hearings and comments filed by a wide range of parties, the Commission concludes that no single technology or method will effectively protect children from harmful material online. Rather, the Commission determined that a combination of public education, consumer empowerment technologies and methods, increasing enforcement of existing laws, and industry action are needed to address this concern".

References

ABDI N. & LAUNET E. (2000), "Un filtre antiporno au banc d'essai - Des chercheurs ont mis au point un logiciel détecteur d'images licencieuses", *Libération – Multimédia*, samedi 11 et dimanche 12 novembre 2000.
http://www.liberation.com/multi/actu/20001106/20001111samzc.html

BANGEMANN M.:
- (1997a), *A New World Order for Global Communications – The Need for an International Charter*, Geneva, 8th September 1997, available on 14/10/97 at http://www.ispo.cec.be/infosoc/speech/geneva.html
- (1997b), *Europe and the Information Society – The Policy Response to Globalisation and Convergence*, Venice, 18th September 1997, available on 14/10/97 at http://www.ispo.cec.be/infosoc/speech/venice.html

Belgian Bill, n° 214, on computer crime. Available at http://www.lachambre.be/cgi-bin/docs.bat?l=f&dir=214

Bertelsmann Foundation:
- (1999) September, *Self-Regulation of Internet Content*
http://www.cdt.org/speech/BertelsmannProposal.pdf or
http://www.stiftung.bertelsmann.de/internetcontent/english/frameset.htm?content/c2200.htm
- (2000), *Workshop 'Self regulation on the Internet: filter systems' September 8th, 2000*, Gütersloh workshop, Final report, available at :
http://www.stiftung.Bertelsmann.de/internetcontent/english/frameset.htm?content/c2430.htm.

BOWMAN L.M. (2000): *Filtering programs block candidate sites*, November 8, 2000
http://www.zdnet.com/filters/printerfriendly/0,6061,2651471-2,00.html

CANNON R. (1996): "The legislative history of Senator Exon's Communications decency Act: regulating barbarians on the Information superhighway" *Fed. Communications Law Journal*, Nov. 96, pp. 49, 51-94.

Centre for Democracy and Technology (CDT):
- (1999): *An Analysis of the Bertelsmann Foundation Memorandum on Self-Regulation of Internet Content: Concerns from a User-empowerment Perspective*, October, http://www.cdt.org/speech/991021bertelsmannmemo.shtml
- (2000a): November 21, *French Court Holds Yahoo Accountable for U.S. Auction Content, CDT Policy Post [distribution list]*, A Briefing On Public Policy Issues Affecting Civil Liberties Online From The Centre for Democracy and Technology, Volume 6, Number 20.
- (2000b) December 18, *Congress passes filtering mandates for schools and libraries, CDT Policy Post [distribution list]*, A Briefing On Public Policy Issues Affecting Civil Liberties Online From The Centre for Democracy and Technology, Volume 6, Number 22.

Charte de l'Internet (1996) : *Proposition française présentée à l'OCDE pour une Charte de Coopération internationale sur Internet*, 23 octobre. available on 4/28/97 at http://www.planet.net/code-interent/Charte.html

Commission of the European Communities:
- (1996a): *Illegal and harmful content on the Internet*, 16 October, Com(96) 487 final (http://www2.echo.lu/legal/en/internet/communic.html)
- (1996b), *Green paper on the protection of minors and human dignity in audio-visual and information services*, 16 October, 1996Com(96) 483.

Commission on Child Online Protection (COPA) (2000): *Report to Congress*, Oct. 20, available at http://www.copacommission.org/report/

Computer Professionals for Social Responsibility (CPSR) (1998): *Filtering FAQ, Version 1.1.1*, 10/24/98, written by HOCHHEISER H., http://quark.cprs.org/~harryh/faq.html

Council of Europe:
- (1995a): *Recommendation N° R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology*, adopted on 11 September 1995, http://www.coe.fr/cm/ta/rec/1995/95r13.htm
- (1995b) *Recommendation N° R (95) 19 of the Committee of Ministers to Member States on the Implementation of the principle of subsidiarity*, adopted on 12 October, http://www.coe.fr/cm/ta/rec/1995/95r19.htm
- 4.XI 1950, European Treaty Series - No. 5, Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, Rome, http://conventions.coe.int/treaty/en/WhatYouWant.asp?NT=005
- (2000) 2 October, *Draft Convention on Cyber-crime* (Draft N° 22 REV. 2) http://conventions.coe.int/treaty/EN/cadreprojets.htm

Council Decision of 29 May 2000 to combat child pornography on the Internet, *Official Journal*, L 138, 09/06/2000, p. 1, http://europa.eu.int/eur-lex/en/lif/dat/2000/en_400X0375.html

Council Recommendation of 24 September, 1998 on the development of the competitiveness of the European audio-visual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (98/560/EC) - L 270/48-55 *Official Journal of the European Communities.*

CUSTOS D. (1998), "Liberté d'expression des adultes et protection des mineurs sur le réseau internet selon la Cour suprême des Etats-Unis", *Rev. Dr. Public*, T. 53, 6, p. 1637 and ff.

CRANOR L. F., RESNICK P. & GALLO D. (1998): *Tools at a Glance*, http://www.research.att.com/projects/tech4kids/ToolTable.html

Departments of Labor, Health and Human Services, and Education, and related Agencies, H.R.4577- Appropriations Act, 2001 (Reported in the House), available at http://www.thomas.loc.gov/cgi-bin/query/D?c106:1:.:temp/~c106qYRg1a:64959

European Commission (1998): Directorate-General XIII, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM(98)50, The need for strengthened international co-ordination*, http://europa.eu.int/ISPO/eif/policy/com9850en.html

European Parliament and Council:
- (1999): *Decision N° 276/1999/EC of the European Parliament and of Council of 25 January 1999 adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, see http://www2.echo.lu/legal/en/iap/decision/ or http://www.ispo.cec.be/iap/
- (2000): "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')", *Official Journal*, L 178 , 17/07/2000 p. 0001 - 0016 http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html

European Union:
- Internet Action Plan (IAP), http://europa.eu.int/ISPO/iap/
- Internet Action Plan (IAP), *Filtering Software and Services - Benchmarking study, call for proposals*, IST 2000 conference in Nice, France (6 - 8 November) full text of announcement. See http://www.qlinks.net/iap/

FINKELSTEIN S. (2000): SmartFilter's Greatest Evils - An anticensorware investigation, November 16, http://sethf.com/anticensorware/smartfilter/greatestevils.php

First World Summit for Regulators, 30 November - 1 December 1999, Paris, UNESCO: Statement and Action Plan, Synthesis (30 p.)

FRYDMAN B. (1997) : Quel droit pour Internet ? in *Internet sous le regard du droit*, Ed. du Jeune Barreau de Bruxelles, Brussels, pp. 279-316.

GetNetWise at http://www.getnetwise.org/ or http://www.SafeKids.com/filters.htm.

GUERNSEY L. (2001): January 3, Yahoo to Try Harder to Rid Postings of Hateful Material, *The New York Times on the Web,* http://www.nytimes.com/2001/01/03/technology/03YAHO.html

GIDARI A. (1998): "Observations on the State of Self-Regulation of the Internet", Prepared for The Ministerial Conference of The Organisation for Economic Co-operation and Development ("OECD"), *A Borderless World: Realising the Potential for Global Electronic Commerce Ottawa*, Canada October 7-9, 1998, see http://www.llpf.org/selfreg/whitepaper.htm.

Global Internet liberty Campaign (GILC) (1998): September, *Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet*, http://www.GILC.org/speech/report/

GRAINGER G. (1999): *Broadcasting, co-regulation and the public good*, World Summit for Regulators 30 November- 1 December, Paris, UNESCO.

HOFF O.K. (2000): *Self Regulation of Internet Content 'Filter Systems'*, Presentation ICRA, Gütersloh Workshop, 8th September. http://www.stiftung.bertelsmann.de/internetcontent/english/download/prof_okh.htm

Hong Kong Internet Service Providers Association (HKISPA) (1997): September, Code of Practice - Practice Statement on Regulation of Obscene and Indecent Material, http://www.info.gov.hk/tela/f_care.html

ICRAsafe, http://www.europa.eu.int/ISPO/iap/projects/icrasafe.html

Internet Content Rating Association (ICRA), http.//www.icra.org

Internet Crime Forum IRC sub-group (2000): October, *Chat Wise, Street Wise – children and Internet chat services*, http://www.internetcrimeforum.org.uk/

Internet Industry Association:
- December 1999, Internet Industry Codes of Practice – Codes for Industry Self Regulation in areas of Internet Content pursuant to the requirements of the Broadcasting Services Act 1992 as amended, available at http://www.iia.net.au/code6.htm.
- December 16, 1999 – updated 22 December, IIA Guide for ISPs – internet content regulation checklist, available at http://www.iia.net.au/guide.html
- December 20, 1999 – updated February 2000, Guide for Internet Users – information about online content, at http://www.iia.net.au/guideuser.html

Ipsos-Reid (2000): November 20, *American Kids Spend Most Time Online But More Likely To Face Content Restrictions From Parents,* http://www.angusreid.com/media/content/pdf/mr001119_2.pdf

JANSSON E.L.O. & SKALA M. (2000): The Breaking of Cyber Patrol ® 4, 03/11/2000 In the past, available at http://www.openpgp.net/censorship/cp4break.html

JULIA-BARCELO R. & KOELMAN K.J. (2000): "Intermediary liability in the e-commerce directive: so far so good, but it's not enough", *Computer Law & Security report*, vol. 16, n°4, pp. 213-239.

KATSCH E (1996): Dispute Resolution in Cyberspace, Connecticut, *Law Review*, 28, 953 and ff.

KERR D. (2000): *Action Plan on promoting safer use of the Internet - Self labelling and Filtering,* INCORE Final Report, http://www.ispo.cec.be/iap/ and http://www.incore.org/full.pdf

KOELHMAN K.J. (2000): "Online Intermediary Liability", in B. Hugenholtz (ed.), *Copyright and Electronic commerce*, Kluwer.

KONRAD R. (2000*): New filter scours servers for illicit content*, 24 October, see http://news.cnet.com/news/0-1005-200-3277835.html?dtn.head

LAUNET E. (2000) : Des parents hors ligne – Sondage Ipsos – *Libération* Powow.net, *Libération Multimédia*, 17 novembre, http://www.liberation.com/multi/actu/20001113/20001117venze.html

LEBIHAN R. (2000): Australian controversy over government Web censorship, 3 July, http://zdnet.co.uk/news/2000/26/ns-16352.html

LESTER A. (1993): "Freedom of expression", in MacDonald, Matscher, and Petzold, *The European system for the protection of human Rights*, Martinus Nijhoff Publishers, Amsterdam.

LIIKANEN E. (2001): (Member of the European Commission responsible for Enterprise and theInformation Society), *Better Regulation: from Principles to Practice,* Alternative Regulatory Models Conference Brussels, 6 February, http://www.qlinks.net/items/qlitem9796.htm

LOUVEAUX S., POULLET Y. & SALAÜN A. (1999): "Consumer Protection in Cyberspace, Some Recommendations", *Info*, n°1/6, pp. 521-537.

MATHONET PH., LAMBORGHINI S. & MARTINOLI M. (1999): *PREPACT – Review of European Third-party filtering and rating software & services* (Lot 3), Final Report vol 1, 66 p., see http://www.ispo.cec.be/iap/.

OECD (Organisation for Economic Co-Operation and Development) (1998): *Conference Conclusions*, OECD Ministerial Conference 'A Borderless World: Realising the Potential of Global Electronic Commerce', Ottawa, 7- 9 October.

OVERELL P. (1996): *NNTP Extension for PICS Newsgroup Rating,* http://www.turnpike.com/ratings/syntax.html

PERRITT Jr HH (1996): Jurisdiction in Cyberspace: the role of intermediaries, in *Symposium on Information, National policies and International Infrastructure,* Harvard, 28-30 January, available at http://www.Law.vill.edu/harvard/article/harv96k.htm

POULLET Y.:
- (June 2000): *Safe Harbor: An adequate Protection ?* http://www.droit.fundp.ac.be/textes/safeharbor.pdf
- (October 2000): "Some considerations on Cyberspace Law", in *The International dimensions of Cyberspace Law,* Ashgate (in association with Unesco), London.
- to be published, *How to regulate Internet: new paradigms for internet governance - Self-regulation: Value and limits*, ECLIP Report, available at the CRID's web site: http://www.droit.fundp.ac.be/crid/

President's Working Group on Unlawful Conduct on the Internet (March 2000), *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet,* A Report of the President's Working Group on Unlawful Conduct on the Internet, http://www.usdoj.gov/criminal/cybercrime/

REIDENBERG J. (1996): *Governing Networks and Cyberspace Rule-Making, symposium on Information, National Policies and International Infrastructure*, Harvard, 28-30 January, http://www.law.emory.edu/ELJ/volumes/sum96/reiden.html

RENO J. (2000): *Reno Address on Cybercrime: Encourages industry and law enforcement agencies to work together,* discourse at the ITAA Cybercrime Summitt, July 28, available at http://uspolicy.usembassy.be/Issues/Ecommerce/Reno.062300.htm

RESNICK P. (1998): *PICS, Censorship, & Intellectual Freedom FAQ,* http://www.si.umich.edu/~presnick/pics/intfree/faq.htm (Version 1.14 last revised January 26, 1998) (date of access 31/05/99).

RYAN M.E. & TRIVERIO J. (1999): *Net Guards: Parental Filtering Software*, http://www.zdnet.com/pcmag/features/utilities99/parfilt01.html

Senate and House of Representatives of the United States of America (1998*): Final joint version of H.R. 2281, DMCA (Digital Millenium Copyright Act),* October 20, Signed into law Oct. 28, 1998 as Public Law 105-304 http://www.eff.org/ip/DMCA/hr2281_dmca_law_19981020_pl105-304.html

The Internet Filter Software Chart, http://www.SafeKids.com/filters.htm

The Censorware Project, A (Not So) Brief History of PICS; Cite as: The Birth of the Global Rating System, http://censorware.org/pics/history (date of access 28/02/2000) http://censorware.org/pics/history/9506_ihpeg_birth.txt

TUROW J. & NIR L. (2000): "The Internet and the family 2000, The View from parents, The View from Kids", May, *The Annenberg public Policy Center of the University of Pennsylvania, report Series* no. 33.

Singapore Broadcasting Authority:
- (1996): *The Singapore Broadcasting Authority Act (Chapter 297) - Internet Code of Practice,* http://www.sba.gov.sg/work/sba/internet.nsf/pages/code
- (1999): *SBA's Approach to the Internet,* http://www.sba.gov.sg/sitemap.htm

TRUDEL P. (1988-1989) : "Les effets juridiques de l'autoréglementation", 19, *R.D.U.S*, pp. 247-286.

Tribunal de Grande Instance de Paris, Ordonnance de référé du 20 novembre 2000, Association "Union des Etudiants Juifs de France", la "Ligue contre le Racisme et l'Antisémitisme", le "MRAP" (intervenant volontaire) / Yahoo ! Inc. et Yahoo France http://www.legalis.net/jnet/decisions/responsabilite/ord_tgi-paris_201100.htm

UDEKEM-GEVERS (d') M. (1999): *Internet Filtering Criteria: Survey and Ethical Stakes*, Proceedings of the 4th ETHICOMP - International Conference on the Social and Ethical Impacts of Information and Communication Technologies, (ETHICOMP99, Look to the future of the Information society, 6 to 8 October 1999, Rome), Luiss CeRSIL, ISBN 88-900396-0-4.

United Nations, *Universal Declaration of Human Rights,* http://www.unhchr.ch/udhr/lang/eng.htm

United Nations, Economic and Social Council (1998):, 28 January, *Promotion and protection of the right to freedom of opinion and expression* - Report of the Special Rapporteur, Mr. Abid Hussain, submitted pursuant to Commission on Human Rights resolution 1997/26, E/CN.4/1998/40, http://www.unhchr.ch/Huridocda/Huridoca.nsf/TestFrame/7599319f02ece82dc12566080045b296?Opendocument

US Report delivered the 9th of March 2000 on controlling crime on the Internet, http://www.usdoj.gov/criminal/cybercrime/unlawful.html

WILDE Mathews (2000): "October 27, Copyright Office backs content holders", *WSJ Interactive Edition*, http://www.zdnet.com/filters/printerfriendly/0,6061,2646075-2,00.html

W3C, *PICS Frequently Asked Questions* (FAQ), http://www.w3.org/2000/03/PICS-FAQ/