

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### Internet content regulation

d'Udekem-Gevers, Marie; Pouillet, Yves

*Published in:*

Computer Law and Security Report

*Publication date:*

2001

*Document Version*

Publisher's PDF, also known as Version of record

#### [Link to publication](#)

*Citation for published version (HARVARD):*

d'Udekem-Gevers, M & Pouillet, Y 2001, 'Internet content regulation: concerns from a European user empowerment perspective about Internet content regulation : an analysis of some recent statements : part 1', *Computer Law and Security Report*, vol. 17, no. 6, pp. 371-378.

#### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# INTERNET CONTENT REGULATION

## CONCERNS FROM A EUROPEAN USER EMPOWERMENT PERSPECTIVE ABOUT INTERNET CONTENT REGULATION: AN ANALYSIS OF SOME RECENT STATEMENTS — PART I

Marie d'Udekem-Gevers and Yves Poulet

This article, to be published in two parts, explores the debate between the Bertelsmann Foundation and the Centre for Democracy and Technology about regulation on illegal and harmful content on the Internet. The authors intend to analyze the method, interests and limits of the self regulatory model proposed by the European institutions, bearing in mind the users' empowerment perspective.

### 1. INTRODUCTION

The 'Internet Content Summit'<sup>1</sup> was organized in Munich on 9-11 September 1999 and funded by the Bertelsmann Foundation in cooperation with Internet Content Rating for Europe (INCORE).

At this Summit, the Bertelsmann Foundation presented the "Memorandum on Self-Regulation". This Memorandum is the central pillar of the Internet Content Summit. It contains key recommendations for the Internet industry, policy makers, law enforcement authorities and users. These recommendations are allegedly based on reports by leading experts<sup>2</sup> from four universities, around the world, and on the Internet User Survey, that was carried out in Australia, Germany and the United States.

In October 1999, the Centre for Democracy and Technology (CDT) published on the Web<sup>3</sup> an answer entitled "An Analysis of the Bertelsmann Foundation Memorandum on Self-Regulation of Internet Content: Concerns from a User Empowerment Perspective." According to this:<sup>4</sup>

The Memorandum's approach would *jeopardize free expression* on the Internet by promoting a single, comprehensive, global rating system developed with government involvement or backed up by government enforcement, and in the name of 'self-regulation,' encouraging ISPs to jointly subscribe to controls over legal content considered offensive by some.

The title of our paper echoes the title of the CDT paper.

Our first aim is to analyze and add some nuances to the CDT text. Here, other points of view will be taken into account. This could help to enlighten the very heated debate on Internet content regulation.

*Secondly and more fundamentally, we would like to emphasize the crucial point of the debate between the two*

*protagonists mentioned. What is the best way for regulating the Internet content? Self-regulation contrasts with traditional public regulation. The OECD inter-ministerial Conference of Ottawa held in October 1999 proposed a third way: the 'co-regulation' or the 'effective mix' between self-regulation and public intervention. This third approach seems to have received great support over the last two years.*

Apart from this first sketch of the context, we propose the following table of contents: our analysis starts by giving information about the authors of the two previously mentioned texts (CDT and the Bertelsmann Foundation). We continue by analyzing the fundamental concepts as regards the different regulatory approaches and the objects of this regulation. Then we try to pinpoint the players and the main considerations of Internet regulation and we focus on the concept of 'user empowerment'. Subsequently, we suggest an analysis of the main European official texts about content regulation on the Internet: we underline that they show an evolution. At this stage, we are ready to comment, in detail, on the two parts of the CDT text criticizing the Bertelsmann Foundation Memorandum: "Promoting a single, comprehensive, global rating system" and "Encouraging ISPs to jointly subscribe to controls over legal content." Within this context, we will give details of the current filtering activities and propose certain classifications as regards the various filtering and rating activities before concluding with the respective roles of the public authorities and of the private sector.

But before any further analysis, we would like to underline that the central concept and word 'labelling' is considered here as synonymous with 'rating'. We would like also to emphasize that both these words will be used in our text with two different meanings. On the one hand, we will speak about the labelling (or rating) of *Internet content* which can be used by

a *technical filter* to control the access to this content (see § 7.1) and are usually not made to be seen by people. On the other hand, we will also mention labels i.e. logos used as quality certification to be read *by people* to evaluate a *service or a product* (see § 3.1). Of course, visual logos can certify that content has been electronically rated to be technically filtered.

## 2. WHO'S WHO?

As the starting point of our discussion, we will introduce the authors of the documents in question: the CDT and the Bertelsmann Foundation.

### 2.1 Center for Democracy and Technology

As explained on its home page, the Center for Democracy and Technology (CDT), located in Washington DC, is "a non-profit public policy organization dedicated to promoting the democratic potential of today's open, decentralized, global Internet." Its mission "is to conceptualize, 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 organizing with the Internet user community and public education campaigns, and litigation, as well as through the development of technology standards and online information resources."<sup>5</sup>

### 2.2 The Bertelsmann Foundation and several of its links

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.<sup>6</sup>

One should note that this foundation has started by the eponymous media giant, which is also AOL's partner in Europe.

As previously noted, the Bertelsmann Foundation in association with INCORE organized the Munich Summit. "INCORE (Internet Content Rating for Europe) was set up by a group of European organizations with a common interest in industry self-regulation and rating of Internet content. It is now focused on a project, which aims to create a generic rating and filtering system suitable for European users. This is being funded by the European Commission in 1999."<sup>7</sup> "The original core partners of INCORE are leading related projects on:

- Rating and filtering - Internet Watch Foundation (IWF)
- Usenet News - Electronic Commerce Organization (ECO)
- Hotline development - Childnet International (INHOPE)."

Notably Microsoft and UUNET® sponsor INCORE.<sup>8</sup>

Moreover, 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, is a member of the Internet Content Rating Association (ICRA). ICRA "was formed in April 1999 as an independent, non-profit organization. [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. The Recreational Software Advisory Council has formally folded into ICRA which now manages and operates the RSACi rating system. [ICRA is] planning an extensive, international consultation exercise to consider what other categories of content to include in a revised system to be launched in mid 2000."<sup>9</sup>

There is no doubt that, in any discussion about Internet regulation and beyond some so-called 'non-profit organizations', the economic and financial considerations involved are both enormous and worldwide! As a point of information, we note that, according to Konrad (2000), the marketing consulting company Frost and Sullivan estimates that the "US market for Internet filtering software will be US\$1.5 billion in 2004."

## 3. HOW TO REGULATE INTERNET AND WHAT TO REGULATE?

### 3.1 How to regulate Internet

There are three Internet regulation paradigms: self-regulation, Government regulation and co-regulation.<sup>10</sup>

#### Self-regulation (or private regulation)

Self-regulation is a private norm, i.e. that the norm is enacted by private bodies. Therefore, it stands in contrast to a public or governmental norm which is enacted by public authorities in the limits and under the basis of 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<sup>11</sup> 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 due to 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 more and more encompasses a set of structured norms included within codes of conduct or codes of practices<sup>12</sup> 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'* remind strangely of vigilante justice. New ways of enforcement have been set out in the last few years in the context of the fight against illegal or harmful content on Internet.

The *hot lines* created by certain codes of conduct to enable the condemnation of activities contrary to that code, represent another example of the means set up to ensure adherence to network discipline. Some systems like the *quality labelling*<sup>13</sup> 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 as regards websites of journalistic information referring to respect of the press code) are of greater interest. Obviously, the value of such a certification depends on the quality of the certifying body that defines, issues and controls it.

Furthermore, there are different initiatives for the creation of *'virtual magistrates'*,<sup>14</sup> online arbitrators or mediators who are authorized to adjudicate conflicts arising out of network use, whether they be issues of defamation, intrusion of privacy or non-respect of the rules of a news group. Such Alternative Dispute Resolution (ADR)<sup>15</sup> mechanisms have been recently promoted by the European directive on certain legal aspects of Electronic Commerce in the internal Market.<sup>16</sup>

Thus, we can see that private regulatory sources establish their own mechanisms for expressing the rules, controlling their application and finally 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 of an international authority. Currently, a few 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<sup>17</sup> 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 License) 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.

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 has been discussed by the Broadcasting Authority with all interested parties before to be enacted.<sup>18</sup>

On the other hand, the international dimension of information superhighways leads States to search, at the international level, for models to develop the law, or for cooperation among the national authorities (Frydman, 1997). Through international conventions,<sup>19</sup> bodies,<sup>20</sup> treaties of police cooperation amongst

States engaged in the fight against cyber-crime and the draft for an International Internet Cooperation Charter presented by France on October 1996<sup>21</sup> to the OECD., a number of public initiatives have been taken to maintain the role of the State in protecting and safeguarding individual rights and public interest. The Council of Europe published on October 2000 a Draft Convention on Cyber-crime.<sup>22</sup> Some go so far as to suggest the creation of an "International Cyberspace Authority", in reaction to movements for the emancipation of Internet law and to the increasing power of private norms. The "new world order for global communications"<sup>23</sup> promoted by the former European Commissioner, M. Bangemann (1997a & b), stressed the importance of setting up this global authority and fixing global rules for electronic commerce.

But, when such a solution is envisaged, the complexity of the functioning of the 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 activity is growing.

### '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, discussed in depth the idea of combining the two previous regulatory approaches in a co-regulatory effort of both private and public partners. The main idea is 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<sup>24</sup> 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) or as a way to guarantee the effective sanctions of private regulations (see e.g. the US Privacy Safe Harbor Principles<sup>25</sup> whose effectiveness 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 deceptive statements, precisely in a case the fact 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 fixed following the so called 'subsidiarity principle'.

As regards the division of responsibilities between the public and private regulatory interventions, we see the subsidiarity principle as an hermeneutic key principle to fix the boundaries of the different regulatory techniques and bodies including the self-regulatory ones.<sup>26</sup> In other words, everything you can fix by self-regulatory solutions must be fixed by self-regulatory solutions.

The cooperation and dialogue between private and public regulations are now usually considered<sup>27</sup> as the best way to effectively ensure public interest objectives, in the full respect of the balance embedded in our legislation and international Conventions. That is why we might consider co-regulation as integrated effective mix between public and private regulation.

In § 8.2, we will return to the concept of co-regulation to try to analyze 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 contents have 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).

## 4. PLAYERS AND CONSIDERATIONS OF INTERNET CONTENT REGULATION

### 4.1 Players of Internet content regulation

Actors implicated in Internet content regulation are numerous: on the one hand, they are providers and, on the other hand, customers of this regulation.<sup>28</sup>

Among the providers, several are ‘traditional’ in the Internet domain: Internet access providers (I.A.P.) (who allow to access to Internet and its basic services (E-mail, Web, news)), Internet service providers (ISP) (who offer complementary services, including hosting<sup>29</sup>), telecommunication companies (including network operators), multi-media and content providers (e.g. media and publishers).

The other providers are more recent 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. In the future, the list of those players would be longer and also include: label distribution services, bodies

in charge of setting filtering criteria (i.e. customizing) and, possibly, services dedicated to installing/running filtering software, (see the six roles implicated by any filtering software according to Resnick 1998).

And last but not least in the list of players, there are the customers of Internet content regulation services 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.

### 4.2 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 individual providers outlined in § 4.1. Indeed, selling new products or services related to the Internet content control might interest some traditional providers (see § 4.1). Furthermore, content providers or ISP’s might consider that a *quality label* gained by the use or the offer of these filtering or rating systems might be a good argument as regards the *marketing* of their products.

Another economic dimension should not be underestimated: the recent *judgements against web host providers which have hosted illegal websites*<sup>30</sup> have created an increasing fear among these providers as regards the economic consequences of these decisions and the will to find adapted solutions (including the use of techniques selecting or at least scanning the content) put at the disposal of their customers.

On the other hand, at a more macroeconomic sub-level, the case already discussed in § 2.2 of the ICRA association makes clear that the: ‘world’s best known Internet and communications companies’ are greatly interested in joining to try to *control Internet regulation*. Since the growing economic importance of the Internet phenomenon, there is a risk that financial considerations of Internet regulation are the most important and somewhat eclipse the others.

The top level (see Table 1 below) 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

**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 case of value conflict, which one(s) prioritize?
Level 2: societal & political considerations	How to implement the promotion of chosen values? Who is responsible for the child protection?
Level 1: financial & economic considerations	How to preserve the interests of the various providers involved?

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,<sup>31</sup> can be outlined. So far it is quite obvious that the different values enumerated are in conflict with each other, e.g. the freedom of expression principle will clearly restrict any forms of control of the web sites, control which might be justified for reason of protection of minors. In case of value conflict, which one(s) do we prioritize? The entire problem is thus to strike an appropriate balance between these contradictory values. This is clearly formulated in the following key 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 is one issue. Particularly, who (State / Internet service providers / Content providers / Parents / Schools) is in charge of child protection?

## 5. THE CONCEPT OF 'USER EMPOWERMENT'

CDT uses the concept of 'user empowerment' as the reference in its analysis of the Bertelsmann Foundation Memorandum. As defined by CDT: "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." (CDT, 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 agree with filtering, they have to choose which kind of filtering they need.<sup>32</sup>

As to the Memorandum, it also endorses the concept of user empowerment, considering (p. 10) self-rating and filtering systems as 'empowering user choice'.

Historically, the concept of 'parent empowerment' linked to Internet governance appeared in the US from 1995 as an Internet software industry reaction to the threat of government censorship. So notably, 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.<sup>33</sup> In August 1995, IHPEG was incorporated into the World Wide Web Consortium (W3C).<sup>34</sup> Nevertheless, on February 8 1996, Senators Exxon and Coats' Communications Decency Act (CDA), was signed by Clinton. CDA: "made it illegal knowingly to provide indecent or manifestly shocking material to minors via electronic computer networks."<sup>35</sup> The industry reacted in two ways:

- First, a coalition of publishers, material providers, access providers and civil liberties associations attacked the legislation, claiming it invalidated the First Amendment.
- Then it stepped up its efforts to find an alternative [technical] solution to legislation....<sup>36</sup>

On 26 June 1997, the US Supreme Court finally declared some of the provisions of the Decency Act to be unconstitutional. The reasoning held by the Court is founded on the finding that the provision providing criminal sanctions for Internet service providers 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 takes also into account the specificity of Internet as media vis-à-vis other ones.<sup>37</sup> Finally, the Court decided that there were other means of control that were less restrictive with regards to freedom of expression.<sup>38</sup>

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 minimize the risks from unlawful conduct involving use of the Internet." Moreover, on 23 October 2000, the US Commission on Online Child Protection<sup>39</sup> claimed (notably p. 9 and 10) that consumer empowerment (pp. 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.

As it will be demonstrated in the next point (§ 6), the *European Union* has fully endorsed the approach of 'empowering parents to protect minors',<sup>40</sup> since the end of 1996. In September 2000, R. Swetenham of the European Commission<sup>41</sup> developed this concept, outlining the three pillars of Internet Content Regulation: "Freedom of choice, control and information : first freedom of choice for the user to determine himself which Internet content he or his children can use; second control over access to Internet data that should be vested in the user rather than in any governments; and finally information to support the user in making responsible use of the Internet."

This 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 1001 US parents with at least one child (between ages eight 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<sup>42</sup> (by Ipsos "Libération" and Powow.net) 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%) mainly fear pornography. 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 but 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<sup>43</sup> should be primarily responsible for preventing child access to some websites.

Finally, it is worth noting that, according to the conclusion drawn by Morawski<sup>44</sup> 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."

## 6. MAIN EUROPEAN UNION OFFICIAL TEXTS ABOUT INTERNET CONTENT REGULATION

The Bertelsmann Foundation Memorandum, which is criticized by CDT, lies within the scope of European Union politics. Before any discussion, let us thus recall several relevant excerpts from the main European Union official texts about 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 emphasized the evolution of these successive texts as regards the responsibilities for controlling Internet content.

### 6.1 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'<sup>45</sup> and 'Illegal and harmful content on the Internet'.<sup>46</sup> 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*<sup>47</sup> standard or equivalent systems...

Thus the European texts unambiguously support the leadership of the private sector (as in the case of the US<sup>48</sup>). 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]

### 6.2 The second trend (1998-1999): encouraging private-public cooperation

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."<sup>49</sup> 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 online services.

Let us underline that this text shows an evolution<sup>50</sup> 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 that must be set up, drafted, implemented and evaluated by all actors interested in this regulation. Thus the industry will have to work together with representatives of consumers, civil liberties' associations, privacy authorities and definitively with official authorities in charge of the prosecution of crimes.

In the same trend as this Council Recommendation, let us still note the 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."

"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).

It should be noted that the Bertelsmann Foundation Memorandum dates back to 1999 and conforms to the underlined trend of the European official text for this period 1998-1999: it suggests a private-public cooperation (see § 8.1). And it is also worth pointing out that this Memorandum contributes to the trend that follows, as explained in next paragraph.

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

The Council decision to combat child pornography on the Internet adopted on 29 May 2000, after a Parliamentary report prepared by the Citizen's Freedoms and rights Committee based on an Austrian initiative, inaugurates a third trend granting more investigatory 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 *IAP or other Information Society Service Providers to retain traffic-related data* so that the data could be made available for inspection by criminal authorities;<sup>51</sup> to *check the identity of persons who obtain an electronic 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 duty of a large number of information services providers (not only the IAPs or hosting services but also the certification authorities, the trusted third parties or key recovery agents) to cooperate might be viewed as a compensation to the legitimate use of cryptography and other anonymity techniques in order to create a good 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,<sup>52</sup> which includes this duty of cooperation.

At the same time, the adoption of the European Parliament and Council E-Commerce Directive of 8 June 2000 must be underlined. Article 15 of this Directive states that Member states *may not impose on intermediaries a general obligation to monitor third party information they transmit, distribute or store*. Furthermore, article 12 recognizes, 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. These important provisions are the

legislative answer to the concerns expressed by Internet actors (especially by the Bertelsmann Memorandum) that ISP's should not be held liable in the case of illegal or harmful content except if 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 recognized as a pillar of the European Union and Market.

**Marie D'udekem-Gevers** Institut d'Informatique, University of Namur, Belgium.

**Yves Poulet** Centre de Recherche Informatique et Droit (CRID), University of Namur, Belgium.

This paper has been produced thanks to a 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)'. The authors thank N. Condon for having corrected their English text.

**In Part II - Promoting a global rating system and ISP controls over legal content.**

## FOOTNOTES

<sup>1</sup> See: <<http://www.stiftung.bertelsmann.de/internetcontent/english/frameset.htm?content/c2200.htm>>.

<sup>2</sup> In fact, the experts have hardly criticized the fact that the final Memorandum were considered representing the faithful outputs of their reports.

<sup>3</sup> See: <<http://www.cdt.org/speech/991021bertelsmannmemo.shtml>>.

<sup>4</sup> See particularly, the 'overview' published by the CDT and available on the web site (quoted here note 7).

<sup>5</sup> See: <<http://www.cdt.org/mission/principles.html>>.

<sup>6</sup> See: <<http://www.stiftung.bertelsmann.de/english/ueberbl/grundl/index.html>>.

<sup>7</sup> See: <<http://www.incore.org/>>. See the report by D. Kerr, 2000.

<sup>8</sup> UUNET® is a WorldCom company that is: "a global leader in Internet communications solutions offering a comprehensive range of Internet services to business customers worldwide." See <http://www.uunet.com/about/>.

<sup>9</sup> <<http://www.icra.org/>>.

<sup>10</sup> See Poulet, 2000.

<sup>11</sup> See Gidari, 1998.

<sup>12</sup> See notably Internet Industry Association, December 1999.

<sup>13</sup> See Louveaux, Poulet & Salaiün, 1999.

<sup>14</sup> See Katsch, , 1996 and Perritt, 1996.

<sup>15</sup> 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 acknowledge the creation and the legal values of these initiatives under certain conditions as regards the independence of the "judges", the procedure followed before these courts and the transparency of their decisions.

<sup>16</sup> Cf. Article 17 of the European Parliament and Council 'directive on

electronic commerce' (2000).

<sup>17</sup> 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.

<sup>18</sup> 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 § 8.2.).

<sup>19</sup> Such as those of the UNO, UIT, WTO, WIPO, OECD.

<sup>20</sup> Such as the G7.

<sup>21</sup> See 'Charte de l'Internet, 1996'.

<sup>22</sup> The Council of Europe in cooperation with the Italian *National Direction Antimafia* has organized a first pan-European Conference about the "Defence of the Society *vis-à-vis* the organized criminality", Caserta, 8-10 sept. 2000.

<sup>23</sup> The Bangemann's suggestion for an 'international charter for global communications' underlining the need for a strengthened international cooperation was made in September 1997. Since then, the European Commission has issued a communication (1998) on the: "The need for strengthened International Coordination" 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.

<sup>24</sup> This summit was organized by the Unesco in cooperation with the Association of National Audiovisual Authority, November 30 and December 1 1999, Paris.

<sup>25</sup> See Poulet, June 2000.

<sup>26</sup> 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 self-regulatory solutions than by legislative ones.

<sup>27</sup> 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 (cf. § 8.2) to this Australian approach.

<sup>28</sup> Another typology of the players can found in Mathonet et al. 1999, vol. 1 p. 13-29.

<sup>29</sup> They are, in this case, called 'web host providers'.

<sup>30</sup> See Julia-Barcelo and Koelman, 2000.

<sup>31</sup> *Ibid.*

<sup>32</sup> See also § 7.3 and, in particular, table 7.

<sup>33</sup> <[http://censorware.org/pics/history/9506\\_ihpeg\\_birth.txt](http://censorware.org/pics/history/9506_ihpeg_birth.txt)>. (Web site visited July 2000 but now deleted).

<sup>34</sup> <<http://censorware.org/pics/history/>> (Web site visited July 2000 but now deleted).

<sup>35</sup> As regards the content of the Decency Act and its main provisions, see *inter alia*, Cannon, Nov. 96.

<sup>36</sup> Com(96) 483 Annexe IV p. 3.

<sup>37</sup> Two main characteristics define the originality of Internet as a media 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.

<sup>38</sup> *Reno v ACLU*, 117 S.Ct 2329, 65 USLW 4715. About this decision and its reasoning, see Custos, 1998.

<sup>39</sup> See also § 8.2.

<sup>40</sup> See Com(96) 487 final, p. 19.

<sup>41</sup> See Bertelsmann Foundation, 2000.

<sup>42</sup> See Launet, E., 2000.

<sup>43</sup> Several techniques (such as for verifying age), suggested by the US Commission on Child Online Protection (2000, p. 45-46), can be used by content providers.

<sup>44</sup> See Ipsos-Reid, 20 November 2000.

<sup>45</sup> Com(96) 483.

<sup>46</sup> Com(96) 487 final.

<sup>47</sup> See § 6.1.

<sup>48</sup> 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.

<sup>49</sup> 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.

<sup>50</sup> 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."

<sup>51</sup> National legislation has 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.

<sup>52</sup> 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.

## BOOK REVIEW

### EC Law

**Law of the European Community, 2<sup>nd</sup> Edition, by Christopher Vincenzi, 1999, soft-cover, Financial Times Pitman Publishing, 318 pp., ISBN 0 273 63846 7**

This updated new edition of the law of the European Community is intended to provide students with a basic grounding in the principles of EC law. The work provides an account of Community institutions and the general principles of EC law at an introductory level; offers a selection of substantive topics in areas of law such as the free movement of persons, goods and services, and competition law; and provides the reader with an appreciation of the extent that EC law is integrated within the UK legal system. It also considers how EC law has developed to give effect to Community rights. This latest edition, published in 1999, anticipates ratification of the treaty of Amsterdam and describes developments toward economic, political and monetary union that have impinged on EC law. More emphasis has also been given to substantive aspects, including EC trade decisions on free movement of goods, as well as expansion of the section dealing with free movement of goods and intellectual property.

**Available from Pearson Education Ltd, Edinburgh Gate, Harlow, Essex, CM20 2JE; Internet: <[www.pearsoneduc.com](http://www.pearsoneduc.com)>.**