Centre Perelman
de philosophie du droit

Université Libre de Bruxelles

http://www.philodroit.be

Public strategies for Internet Co-Regulation in the United States, Europe and China

B. FRYDMAN, L. HENNEBEL, G. LEWKOWICZ

Série des Working Papers du
Centre Perelman de philosophie du droit
n° 2007/6

Comment citer cette étude ?
B. FRYDMAN, L. HENNEBEL, G. LEWKOWICZ, *Public strategies for Internet Co-Regulation in the United States, Europe and China*, Working Papers du Centre Perelman de philosophie du droit, n° 2007/6, http://www.philodroit.be

Public Strategies for Internet Co-regulation in the United States, Europe and China

By B. FRYDMAN, L. HENNEBEL and G. LEWKOWICZ

Internet defies the classic State law model according to which the sovereign State makes and enforces the law on its territory, including by the use of force (Frydman 1997 ; Svantesson 2005). The required bond between State sovereignty, national territory, and law is loose when dealing with Internet regulation. In addition, international law does not answer the question of which court should have jurisdiction over Internet litigation and what law should be applied (Berman 2002; Svantesson 2005). In other words, Internet engages regulators to use new methods of drafting and implementing legal rules. Co-regulation is one of the techniques that can be used. Despite the fact that defining "co-regulation" remains challenging and unsettled (Lievens *et al*. 2006; Hennebel & Lewkowicz 2007: 148-157; Poullet 2004), one may provide a theoretical sketch of what the co-regulation model entails.

For analytical purposes, it is convenient to make a distinction between regulators and what Zittrain (2003) called "points of control". Regulators are public or private bodies willing to influence the behaviors of actors in a field of action. Points of control are any public or private actors that, for any reason, play a strategic role in a particular area. Regarding Internet regulation, the method used by regulators consists in leaning on these points of control as regulatory levers. The so-called co-regulatory mechanism must be understood in this paper as a legal device designed to put pressure on the points of control to achieve some regulatory result.

The meaning of co-regulation is twofold. As a concept of legal theory, "co-regulation" is a legal model in which the norms drafting, implementation and enforcement is not under the sole authority of the sovereign ruler, but rather spread, voluntarily or not, amongst a number of players both public and private. In a more rigorous sense, co-regulation embraces a new form of governance for public authorities (Schultz & Held 2004), based on the voluntary delegation or transfer towards private actors of the burden of all or part of the drafting, implementation and enforcement of norms.[1] This chapter refers mainly to this latter meaning of co-regulation, focusing on the strategies initiated by States.

In any case, one must tell apart the co-regulation from the *regulation model* – the so-called "command and control" model – in which public authorities make the rules, enforce them and punish those who breach them. Co-regulation is also different from the *self-regulation model* in which the players of a certain sector of activity make the rules and implement them collectively without any public intervention. Still, co-regulation is not just an "in between" model. Co-regulation is a legal model *per se* with its proper rationale based on the empowerment of actors to control one another.

The notion of co-regulation has been used with some success in the context of Internet regulation because of what was called "a move to the middle," that is, an ever increasing role of intermediaries in regulation (Palfrey & Rogoyski 2006; Kerr & Gilbert 2004). It has also been used in the regulation of other media (Hans-Bredow-Institut 2006) as well as in other areas such as corporate governance, corporate social responsibility (Berns *et al*. 2007) and environmental law. It may be seen as a general paradigm for global governance in the context of globalization (Frydman 2004).

So far, most of the academic publications dealing with Internet co-regulation mainly focused on the question of effectiveness of such a model of regulation. While this chapter describes and scrutinizes

[1] Co-regulation in this sense refers to the main alternative mode of regulation as used and defined by the European Union (Palzer 2003; Senden 2005).

the legal initiatives and set of tools developed by the United States, the European Union and China that entrust points of control to monitor Internet, it focuses more specifically on the impact of co-regulation on the rule of law[2]. It shows the emergence of different systems of Internet regulation having an effect on international legal competition and compliance with the rule of law.

X. 2 The United States of America: self-regulation with a taste of co-regulation

The American system of Internet regulation has often been described as self-regulatory,[3] as opposed to the European system (Kesan & Gallo 2006; Chen 2004; Nguyen 2004). However, the American system is not exclusively self-regulatory. Actually, because of a distinct legislative and legal history (Zittrain 2006: 253), the regulatory rationale of the Internet in the United States takes the shape of a self-regulatory system based on a libertarian framework (1). However, it is also in the United States that co-regulatory mechanisms were first outlined to protect specific rights (2).

X.2.1 The American libertarian framework of Internet regulation

Traditionally, United States law distinguishes between the liability of the publisher and of the distributor of litigious information. On the one hand, it engages the liability of the producer of unlawful information with that of the one who publishes the information. On the other hand, it immunizes the booksellers, libraries, and other distributors insofar as they are unaware of and do not have reason to know about the offence (Lichtman & Posner 2006). American courts applied this principle to the Internet in the first lawsuits involving ISPs.[4] However, in 1995, the Supreme Court of the State of New York adopted a different position in the *Stratton Oakmont, Inc. v. Prodigy Services Co.* case.[5] It held that when an ISP takes measures in order to monitor on-line content, it shall be regarded as a publisher. Hence, its liability could be involved. As a consequence, the paradox was that ISPs that had an editorial control policy were more at risk than the ones doing nothing in this respect.

According to the ISPs, this situation would end up undermining the system of Internet self-regulation and appeared likely to open the door to a mass of lawsuits and actions against them that could be a serious obstacle to the expansion of the digital economy. As early as 1996, the U.S. Congress reacted by passing the Communication Decency Act (CDA). Section 230 sets up the so-called "safe harbors" which immunizes all ISPs from any civil liability regarding the material made by others that they only stored or disseminated. Section 230 § 1 c) states that "No provider or user of an interactive computer service shall be treated as publisher or speaker of any information provided by another content provider."[6] The U.S. courts have applied this provision extensively. According to these rules, the hosting provider would not be held liable: 1.) even if it was aware of the unlawful character of the content; 2.) even if it had been notified of this fact by the victim;[7] and 3.) even if it had paid for the illegal data.[8] In addition, section 230 § 2 a), states that

> No provider (…) of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider (…) considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected,[9] and of any action taken to

[2] On Internet regulation and the rule of law, see also Marzouki (2006).

[3] On Internet self-regulation see the study by Price & Verhulst (2005).

[4] For example, in a textbook case, the District Court of New York refused to hold the technical intermediary liable for defamatory comments broadcast via its equipment. See *Cubby, Inc. v. Compuserve, Inc.*, 776 F Supp. 140 (S.D.N.Y. 1991).

[5] *Stratton Oakmont, Inc.* v. *Prodigy Services Company*, 23 Media L Rep (BNA) 1794 (N.Y. S. Ct. 1995)

[6] 47 U.S.C. § 230 (c) (1)

[7] For a defamatory case, see *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997). For a case dealing with advertisement for child pornography, see *Doe v. America Online, Inc.*, 783 So.2d 1010 (FL. 2001).

[8] For a defamatory case, see *Blumenthal v. Drudge and American Online, Inc.*, 992 F. Supp. 44 (D.D.C. 1998). In this case, the defamatory statement was not anonymous but sent by a person with whom AOL contracted and paid a monthly fee.

[9] 47 U.S.C. § 230 (c) (2) (A)

enable or make available to information content providers or others the technical means to restrict access to material.[10]

This latter clause called the "Good Samaritan Provision" shields ISPs which voluntarily monitor Internet content and filter or restrict access to illegal, harmful or "problematic" material. In sum, these provisions shelter ISPs from any tort-based lawsuit whether they decide to do nothing or to edit problematic or controversial content (Frydman & Rorive 2002b: 50; Rustad & Koening 2005). However, the immunity granted by the CDA covers only civil liability and does not extent to criminal law. On the contrary, the CDA intended to criminalize the dissemination of any obscene or indecent message with full knowledge to minors of less than eighteen years of age,[11] although affirmative defenses were provided for those who, in good faith, take effective action to restrict access to minors.[12] These provisions created a kind of mandatory self-regulation which could have been the basis of a co-regulatory system. Nevertheless, the Supreme Court of the United States struck down these criminal provisions and applied the full protection of the First Amendment to Internet content.[13] Despite the drafting of the Child Online Protection Act (COPA) – which called for a similar mechanism to the one judged unconstitutional by the Supreme Court – the Court's ruling was reaffirmed.[14]

The conjunction of a *safe harbor* and Good Samaritan clause provided by the CDA on the one hand, and the full protection offered by the First Amendment to Internet content as asserted by the U.S. Supreme Court on the other, characterize the American system of Internet regulation as a system of self-regulation. Indeed, the American Internet regulatory framework, which immunizes ISPs against civil lawsuits, is based primarily on the voluntary ISPs' monitoring and drafting of codes of conduct.

X.2.2 A taste of co-regulation

Although the libertarian framework generally prevailed, American law displays a taste of co-regulation in three important areas: minor's protection and the fight against child pornography, the fight against terrorism and the protection of copyrighted materials. In these areas, various legal patterns illustrate the "invisible handshake" (Birnhack & Elkin-Koren 2003) between the State and private actors such as ISPs enlisted in the implementation of the law.

In the highly sensitive issue relating to minors' protection, initiatives were taken in order to share the burden of regulation with private actors (Wanamaker 2006). First of all, at a criminal level, denunciation was made mandatory by the 1998 Protection of Children from Sexual Predators Act. It compels ISPs with knowledge of facts involving child pornography to report them to a law enforcement agency.[15] Failure to report may result in a fine of up to $50,000 in the first instance and up to $100,000 for any second or subsequent failures. Likewise, statutes such as the 2000 Children's Internet Protection Act (CIPA) – which exposes public libraries at risk of being scratched out of the federal funds recipients if they do not strain and limit access to pornographic material viewed from their computers – were not held to be unconstitutional.[16] Such rules create incentives for ISPs and other Internet players to act as law enforcement authorities by providing information to the government or by restricting access to controversial material.

---

[10] 47 U.S.C. § 230 (c) (2) (B)

[11] The protection of minors against pornographic material published online is one of the main political objectives of the Congress in the context of Internet regulation (Wanamaker 2006).

[12] 47 U.S.C.A § 223 (e) (5) (A) (supp.1997). See also *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997)

[13] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997)

[14] The long judicial history of the challenging of the COPA could not be discussed here. The most important US courts ruling are *Ashcroft v. American Civil Liberties Union*, 535 U.S. 564 (2002); *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004); *American Civil Liberties Union v. Alberto R. Gonzales*, March 22, 2007, civil action n.98-5591, *available at* http://www.paed.uscourts.gov/documents/opinions/07D0346P.pdf.

[15] 42 U.S.C. § 13032.

[16] See *United States v. American Library Association, Inc.*, 539 U.S. 194 (2003).

Secondly, in the fight against terrorism, some law enforcement initiatives endow ISPs to monitor Internet communication. According to the Patriot Act – amended by the 2002 Cyber Security Enhancement Act – law enforcement authorities may urge ISPs to disclose information relating to an emergency matter. Moreover, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency," he may pass on the content of a communication to a Federal, State, or local governmental entity,[17] and no cause of action can lie in any court against him for providing the information under such circumstances (Birnhack & Elkin-Koren 2003: 103-105).[18] In this case, ISPs are encouraged to act as law enforcement authorities by enjoying immunity against lawsuits involving privacy and data protection violations.

Finally, in the field of copyright's law, Congress drafted a special liability regime for ISPs (Manekshaw 2005). In 1998, the Digital Millennium Copyright Act (DMCA) enacted in the Copyright Act the so-called Washington agreement between copyright owners and representatives of the e-business industry about infringing material online (Frydman and Rorive, 2002b: 51). According to the DMCA, an ISP that is unaware that it is hosting infringing material and does not take advantage from the infringing activity cannot be held liable. However, when a copyright owner notifies the provider about the infringement, the ISP must remove or disable access to the material within ten days (*notice and take down*); otherwise it could be liable for damages. The ISP must also notify the content provider that it has removed or disabled access to the material.[19] The content provider may then dispute the validity of the notice and send a formal counter notification to the ISP.[20] In that case, the ISP has to inform the author of the complaint that it will put the controversial data back online (*notice and put back*),[21] unless an action is filed against the content provider seeking a court injunction. In this way, ISPs play their part in the regulation of infringing material online. However, thanks to the procedure of notice and counter-notice, they don't have to make decisions on their own in case of disputes.

In conclusion, while the U.S. system of Internet regulation is mainly self-regulatory, it uses some co-regulatory mechanisms to guarantee security (e.g. in the fight against terrorism), specific rights (e.g. in the fight against pedophilia), and to protect specific economic interests (e.g. copyright protection). Nevertheless, in the U.S. model, co-regulation is the exception and aims to achieve very specific goals on certain issues. In Europe though, co-regulation is the general and leading model of regulation of Internet content.

X.3 The European Union: co-regulation as a general paradigm

The European system of co-regulation was set up by the Directive on electronic commerce which came into force in January 2002.[22] The text provides a regime of liability limitations less favorable to ISPs than the U.S.'s immunity clause in the CDA. It also leaves more room for State intervention, a position consistent with the European view of the freedom of speech submitted to certain restrictions, liabilities, and penalties that justify the intervention of public authorities. Besides important differences that arise from its transposition into the domestic law of each Member State,[23] the Directive defines the main components of a general co-regulation model of Internet content and it favors the emergence of professional players entrust to monitor the Internet

[17] 18 U.S.C. § 2702 B.8.

[18] 18 U.S.C. § 2703 e

[19] 17 U.S.C. §512 (g) (2) (A).

[20] To be effective, the counter notification must meet the formal requirements set up by 17 U.S.C. §512 (g) (3).

[21] 17 U.S.C. §512 (g) (2) (B).

[22] Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular, electronic commerce in the Internal Market ("Directive on electronic commerce"), *O.J.E.C.*, L 178/1, 17 July 2000, particularly art.12-15. For a complete analysis of the content of the Directive, see Strowel *et al.* 2001.

[23] For Belgium, for instance, see Montero *et al.* 2004: 81. For the French implementation of the Directive, see Sédaillian 2005. For its implementation in Great Britain, see Hedley 2006.

(1). Nevertheless, the European system may appear *too effective* in its current configuration and lacks the guarantees needed to avoid the risks of massive private censorship (2).

X.3.1 A general co-regulation model: towards professionalization and proceduralization

Like the DMCA and CDA in the U.S., the EU Directive primarily intends to create "safe harbors" for the sake of ISPs. The European approach differs however from the American one in terms of method. Firstly, the EU Directive creates conditional exemptions from liability at both civil and criminal levels. Secondly, whereas the U.S. favors a vertical approach regulating legal issues related to the infringement of a specific right, Europeans chose instead – following the German model[24] – a horizontal approach defining general rules applicable to any kind of illegal or damaging material: not only copyright infringement, but also defamation, disclosure of privacy, hate speech, incitement of violence, hard pornography, pedophilia, etc. The Directive states, as a matter of principle, that ISPs are neither obliged to monitor the information that they transmit or store, nor to actively seek out illegal activities on the network.[25] Nevertheless, Member States may compel ISPs to inform them about illegal data or infringements reported by recipients of their services and the identity of their clients.[26] National courts and administrative authorities may also be entitled by national law to enjoin an ISP to restrict access to or to take down illegal, damaging or infringing material.[27]

Regarding liability, the Directive makes an important distinction between access providers and hosting providers. The access provider is the ISP that provides the user access to the Internet. The hosting provider is the ISP that stores the data provided by a content provider on its server.[28] According to the Directive the access provider will not be liable for the information transmitted if it plays only a passive role as a "mere conduct."[29] With respect to hosting activities, Article 14 of the Directive states that the provider will not be liable for the information stored when it is not aware of the illegal activity and, upon obtaining such knowledge, it acts expeditiously to remove or disable access to the information.[30] This clause implicitly leads to an informal "notice and takedown" procedure which, although not organized by the Directive itself, is left to States or self-regulation.

These provisions frame Internet co-regulation at the European level and leave the door open for subsequent developments. Conditional exemption from civil and criminal liability granted to ISPs seems to be a solid starting point for the development of a system of co-regulation. Immunity, especially when it is subject to certain conditions, works as a covetable carrot that the industry is quite willing to run after. This is also why hosting providers play such an important role in the European model of content regulation, rather than the access providers which enjoy more or less full immunity and therefore feel less pressure to interfere with problematic content. As a result, hosting providers have been unwillingly promoted number one regulators of the information society in Europe (Verdure 2005). In addition, the legal environment designed by the EU Directive entails an increase of power of other actors and intermediaries.

First of all, the informal notice and takedown procedure provided by the Directive creates a major incentive to set a standardized procedure. Indeed, ISPs and hosting providers in particular are eager for a better complaints management mechanism that are lodged from various sources regarding controversial content posted on their servers by their customers. Moreover, a standardized notice

---

[24] Informations- und Kommunikationsdienste-Gesetz - IuKDG vom 22 Juli 1997, *Bundesgesetzblatt*, 1997, Teil I Nr. 52, Bonn, 28 Juli 1997, S. 1870.

[25] Directive on electronic commerce, art. 15.1

[26] Directive on electronic commerce, art. 15.2

[27] Directive on electronic commerce, art. 12.3 and 14.3

[28] The same ISP may of course sell both access and hosting facilities. In each case, the liability of the ISP will be determined according to the service that it performed in the transaction.

[29] This implies that the ISP "(a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission." Directive on electronic commerce, art. 12.1

[30] "(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access of the information." Directive on electronic commerce, art. 14.1.

form would allow the ISP to react to notices more accurately and more quickly. Standardization starts with the establishment of a standard notice form allowing ISPs to clearly identify the complainant, the controversial material, and the URLs where it may be seen. These forms would usually require a formal statement by the complainant certifying the notice to be true and sincere by which the complainant accepts to face the legal consequences of any malicious or wrongful notice. Such a standardization could be achieved in different ways through a professional organization or by each ISP individually, in partnership with public authorities or not, etc.

Second, standard notice and takedown procedures are quite demanding and might deter most average end-users from complaining to ISPs about illegal or harmful material they find online. This situation opens the way to another kind of professional intermediaries between end-users and ISPs, specialized in the processing of notices. Those intermediaries, known as "hotlines", bear a key role in the European co-regulatory landscape. Moreover, they are substantially funded by the European Union both at the European and national levels. Since 1999, the European Union has funded the International Association of Internet Hotlines (Inhope), a network of 25 hotlines in 23 countries world-wide. Inhope is in charge of the transmission of notices to ISPs, the police or Inhope members. Between September 2003 and February 2004, the network claims that it received 106,912 reports, including 54,242 related to child pornography.[31] In 2005, over 534,000 reports were sent to Inhope hotlines. Those reports paved the way for significant actions against child pornography. In Germany, for instance, the so called "Operation Marcy" concerning 26,500 Internet users in 166 countries was initiated after the transmission of a report by Inhope members to the German Federal Police.[32] In the United Kingdom, the Internet Watch Foundation (IWF) – the national hotline – reported that its partnership approach led to a reduction in child abuse content hosted in the UK from 18% in 1997 to 0.4% in 2004. In 2005, over 150 UK citizens were identified and reported to the British police by the IWF, resulting in 14 arrests and the current assistance in over 20 police enquiries.[33]

Third, the notice and takedown procedure provided by article 14 of the Directive calls for public and private Internet watchdogs. Internet watchdogs do not only report complaints made by others. They actively seek the Internet, looking for specific kind of illegal material that they intend to contend with. They are funded either by public authorities or by private parties, such as NGOs or business agencies. As a matter of fact, number of hotlines also acts as watchdogs and *vice versa*. For instance, the German association Jugendschutz, created and funded by public authorities, is actively tracking and reporting cyber hate content to public agencies.[34] Since 2001, 750 extremist web sites were shut down as a result of action taken by Jugendschutz.[35] On October 4, 2002, the International Network against Cyber Hate was created by Jugendschutz and the Magenta Foundation in order to coordinate the international action against hate speech on the Internet. This network of watchdogs actively contributes to increase the notice and takedown practices concerning hate speech.

Finally, one might predict that notice and take down would eventually open the way for Online Dispute Resolution mechanisms (ODR) in order to settle disputes about the validity of the material online.[36] At the moment, the content provider or the petitioner have no other choice than to bring

---

- See http://www.inhope.org/en/news/stats.php?id=200309200402 (last visited on April 7, 2007).
- See http://ec.europa.eu/information_society/activities/sip/news_events/success_stories/index_en.htm (last visited on April 7, 2007).
- See http://www.portal.northerngrid.org/custom/files_uploaded/uploaded_resources/1880/IWFjune06esafety. ppt#16.
- See for instance Jugendschutz im Internet, *available at* http://www.jugendschutz.net/.
- INACH Annual Report, 2005, p.23 *available at* http://www.inach.net/content/INACH-annual-report-2005.pdf (last visited on April 7, 2007).
- Article 17 of the Directive on electronic commerce already provides that the States must favor the "out-of-court dispute settlement," including by electronic means. The use of an online dispute resolution (ODR) system, moreover, would be in conformity with the European Council's policy concerning the settlement of commercial cross-border disputes (Council resolution of May 25, 2000 on a community-wide network of national bodies for the extra-judicial settlement of consumer disputes, *O.J.E.C.*, C 155/1, 6 June 2000).

the case before the judiciary in case of take down or put back. Courts are actually dealing with an increasing number of cases regarding Internet content. However, the courtroom is not always the most suitable place to settle this kind of litigation: judicial proceedings are too lengthy, too expensive, and judges are not necessarily experts in cyberlaw. The standardization of ODR could be the major next step in the development of an efficient European system of Internet co-regulation (Katsh 2006; Schultz 2005: 179-250) under the condition that the fairness of the ODR, which is often an area of dispute (Geist 2001; 2002), is guaranteed.[37]

X.3.2 Dangerous effectiveness

While regulating the Internet appeared unworkable ten years ago, nowadays, the system set up in Europe seems to be quite effective. It is sometimes even overly effective so as to jeopardize freedom of speech and freedom of the press in violation of the principles of the rule of law and more precisely of the European Court for Human Rights' standards, based upon Article 10 of the ECHR. Indeed, Article 14 of the Directive on electronic commerce encourages hosting providers to take down controversial material stored on their servers as soon as they are notified by a public authority, a watchdog, a hotline, a NGO, a person claiming to be injured, or any user alleging the material to be illegal, infringing or otherwise damaging (Frydman & Rorive 2002b). Moreover, the system appears to be quite unbalanced since while article 14 incites hosting providers to take such material down, it doesn't give any incentive to put legitimate content back online. This can be explained by the fact that the Directive does not provide a formal notice and takedown procedure that must be instead set by national regulation or self-regulation.[38] This regulatory pattern has negative side effects. The content provider has no formal right whatsoever to ask for a put back or even to be informed of the takedown. As a result, the ISP must decide for itself whether or not to comply with the notices, the accuracy of which may vary, that it receives on a daily basis. The ISP is then in the position of a judge, if not a censor (Frydman & Rorive 2002b). As a matter of fact, recent academic surveys convincingly demonstrated ISPs' trend, especially in Europe, to take down legitimate content when a complaint is lodged, even when it is based on erroneous or misleading information.[39]

In sum, the European informal notice and takedown procedure appears unbalanced and laid open to massive private censorship. This situation could be solved thanks to a legal procedure of counter notice and put back, similar to the DMCA model. Even better, a well balanced system could be inspired by the Japanese model. Whereas the U.S. copyright statute calls for an immediate takedown but allows the content provider to issue a counter-notice requesting a "put back", the 2001 Japanese statute sets up the so-called "notice, notice and takedown" procedure which requires the ISP to forward the notice to the content provider and wait for an answer before removing the notified data.[40] Such a system, which one might also call "reply and stay up," seems more suitable to take the interests of all sides into account and would relieve ISPs from the burden of making

---

[37] The European Court of Human Rights provides some guidelines to insure the fairness of ODR (Schiavetta 2004).

- In its first report on the Directive's application, the Commission stated that "at this stage [it] does not see any need for a legislative initiative". See *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, First Report on the application of 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)*, COM(2003) 702 final, Brussels, 21.11.2003, p.16. On October 24, 2005, the Commission established an "expert group on electronic commerce" which it could consult, notably, on questions related to "notice and takedown procedures." *Commission Decision of 24 October 2005 establishing an expert group on electronic commerce*, 2005/752/EC, *O.J.E.C.*, L 282/20, 26 October 2005. See also studies on the issue of the "notice and takedown" procedure funded by the European Commission (Rightswatch 2003).
- Various experiments were undertaken by researchers to evaluate the perverse effects of this incentive, in particular, in terms of limiting access to contents on the public domain. The results of these experiments show the tendency of ISPs towards censorship, particularly in Europe, of legal contents on the basis of erroneous information (Ahlert *et al*. 2004; Nas 2004). On private censorship on the Internet, see Kreimer 2006.
- See the Law concerning Limitation of Damages to Specific Telecommunications Service Provider and disclosure of Sender Information, *available at* http://www.isc.meiji.ac.jp/~sumwel_h/doc/codeJ/provider-e.htm.

"rulings" that they have neither qualification nor legitimacy to issue. If such mechanisms could enhance the European system of Internet regulation, some States may, however, favor a system of co-regulation precisely because of its censorship potential.

X.4 China: from authoritarian co-regulation to international struggle for law

Both the American and European systems show that co-regulation is an effective way to regulate the Internet either for specific issues or as a general system. However, co-regulation is nothing more than a method of regulation that may be implemented by any regulators with disputable political agenda. Authoritarian States may use co-regulation to chill free speech, censor the Internet and overpower the media. That is exactly what is happening now in China (1) (Cheung 2006; Lacharite 2002; Qiu 2000; Reed 2000: 459-60), resulting in an international struggle for law in the election of a global standard concerning Internet regulation (2).

X.4.1. The evolving pattern of Internet regulation in China

Chinese authorities monitor Internet communications to restrain controversial political and social discussions. At the same time, Internet is used to disseminate Chinese political propaganda, while preserving business transactions and the expansion of the Internet in the country (Cheung 2006: 1, 3; McGeary 2001: 219). Chinese government has set up a strict control and restriction system of access to the Internet by building a virtual firewall that filters unwanted web sites, such as human rights portals and online newspapers like the New York Times, blocking access to them. Individuals or groups are not allowed to make a direct international connection and all Internet access is controlled by the government (Qiu 2000). However, the technology cannot ensure full control and can be challenged by the use of technology itself. Moreover, the enforcement of State censorship can be made extremely difficult if it has to arrest, prosecute, and condemn every single violator (Lacharite 2002).

China consecutively used two methods to regulate Internet content. First, since 1996, the Chinese government has regulated the Internet through extensive legislation and official decrees (Cheung 2006; Newbold 2003), which prohibit messages and conducts that may harm national security, disclose State secrets, endangers social stability or promotes sexually suggestive material, etc. (Cullen & Choy 2005; Newbold 2003).

In addition, co-regulation mechanisms have been progressively set up to delegate Internet monitoring to private actors and the business sector. In doing so, China has adopted a very effective and cost-efficient scheme of control which combines criminal sanctions and privatized enforcement (Boyle 1997), allying direct control and State censorship with surveillance by non-State actors, including foreign investors (Cheung 2006: 11). For instance, under the State Secrecy Law, a person who puts information on the Internet shall ultimately be held liable for any unlawful dissemination of that information, even though information that is provided to or released on web sites must be checked and approved by the appropriate government authority. ISPs and users must put up management systems and all entities or users that establish chat rooms or network news groups are subject to the examination and approval of government agencies. The providers of Internet services and content are liable for any failure to monitor and supervise electronic activities conducted within their business sphere. The Regulations on the Administration of Business Sites of Internet Access Services,[41] passed in 2002, require ISPs to install tracking software, take surveillance and monitoring measures, report to the relevant authorities when someone uses the Internet for illegal activities, keep records of each user's identity card and history of web sites visited for at least sixty days, and install software to filter out the banned sites that are considered subversive by the government (Newbold 2003). The Interim Provisions on the Administration of Internet Publication of 2002 impose similar requirements on actors in the Internet publishing industry, and various statutes and official decrees confirm that the provider must take steps to ensure an effective control

[41] Regulations on the Administration of Business Sites of Internet Access Services (promulgated by the St. Council, Sept. 29, 2002, effective Nov. 15, 2002), LawInfoChina

over the Internet, such as deleting prohibited content, keeping records, and informing officials of illegal activities (Cheung 2006: 24). Failing to take action is against the law and may result in a fine. Finally, to control foreign investors, China initiated the voluntary Public Pledge of Self-Discipline for the China Internet Industry in March 2002 which requires signatories to "monitor the information publicized by users on web sites according to the law and remove the harmful information promptly", and prohibits "links to web sites that contain harmful information" (Newbold 2003: 507). U.S. Internet majors such as Yahoo! signed the Public Pledge and agreed to contribute to the Chinese government's content control management system of policing Internet messages (Heffernan 2006). While it is unclear whether corporations that do not sign the Public Pledge will still be permitted to operate in China (Cheung 2006: 33), it is interesting that China is using a co-regulatory mechanism to ensure Internet censorship by "inviting" ISPs to organize it themselves. For instance, thanks to this method, the Chinese government was able to convince Google to launch a Chinese censored search engine (Kreimer 2006: 18). American ISPs are willing for business reasons to endorse the role of censor – for example, by signing and implementing the Pledge, but also by selling the technology needed to enforce the Chinese filtering scheme or divulging private information to the Chinese authorities (Newbold 2003: 513; Heffernan 2006). This raises the question of the complicity of Internet corporations with authoritarian regimes.

X.4.2. Ruling the rules: transnational struggle for law

They are however some boundaries in the governments' ability to use co-regulation to outsource the implementation of their national law at least within their own territory. ISPs are indeed global players and governments' law could have network effects. This global situation leads to transnational struggle for law.

For instance, as a reaction to the Chinese government's policy and other authoritative countries around the world (Kremer, 2006: 18), the U.S. Congress is currently considering passing a statute to promote freedom of expression on the Internet: the Global Online Freedom Act. This bill aims at establishing an Office of Global Internet Freedom in charge of drafting a list of "Internet-restricting countries." The Act states in section 201 that a "United States business that creates, provides, or hosts any Internet search engine or maintains an Internet content hosting service may not locate, within a designated Internet-restricting country [any materials] involved in providing such search engine or content hosting service."[42] In addition, Internet companies are compelled not to alter their search engines to "produce different search engine results for users accessing the search engine" from different countries.[43] Although the bill is unlikely to be enacted, it reveals another evolution in Internet regulation: cold war between States through Internet companies. This trend underlines the global "struggle for law" that is currently emerging with each State trying to impose its own standards on the other by using ISPs as soldiers for the defense of national values.

In this context, civil society actors also play a role, for instance, by developing and adopting software, like the Psiphon[44] software funded by the Soros Foundation and the University of Toronto, which enables Internet users in Internet censored countries to access blocked sites. Along the same lines, the Voice of America broadcasting service, funded by the U.S. government, contracted with Anonymizer Inc., producer of a censorship circumvention software, in order to provide Iranian citizens with an access to information censored by their government.[45] NGOs could also take part to the judiciary constituent of the international struggle for law. For instance, in April 2007 the U.S. based NGO "World Organization for Human Rights" filed a major lawsuit against Yahoo! based on the Alien Tort Claims Act in an U.S. District Court accusing the Internet

---

- *Global Online Freedom Act of 2007*, H.R. 275, January 5, 2007, sec.201 *available at* http://thomas.loc.gov/cgi-bin/query/F?c110:1:./temp/~c110yo5Bpm:e388.
- *Ibid.*, sec.202.
- Psiphon is an activist software developed by the Citizen Lab. It is described as "a censorship circumvention solution" and contributes, of course, to the global struggle for law in contributing to getting around some national regulations. See http://psiphon.civisec.org/ (last visited April 7, 2007).
- See http://www.anonymizer.com/consumer/media/press_releases/02012006.html (last visited April 7, 2007).

corporation of having aiding and abetting the Chinese authorities to arrest and torture a Chinese journalist. According to the petition, Yahoo! divulged, at the request of the Chinese authorities, the name of the journalist who was using an Yahoo! Internet account to disseminate his calls for democracy in China. Such transnational litigation could add some pressure on ISPs' shoulders and incite them to show more respect towards basic human rights and democratic standards of free speech.

X.5 Internet co-regulation and the rule of law

The paper showed the differences between the regulatory solutions endorsed by American, European and Chinese regulators. In each case, some legal devices were implemented in order to press ISPs to control the Internet. In the US, the co-regulatory model remains exceptional and is used only to achieve very specific goals, while in Europe and China, co-regulation is the general and leading model. If it is quite clear that despite controversies concerning State's ability to control the Internet, States are fully aware of the effectiveness and power of co-regulatory techniques, co-regulation may jeopardize fundamental freedoms and basic guarantees of the rule of law. The paper underlined the Chinese use of co-regulation to support authoritarian policies, and showed that the European system itself was far to be perfect and lacked the necessary safeguards mechanisms required to ensure the full respect of the guarantees of the rule of law. Behind this, one can witness, in the absence of global standards to regulate the Internet, a frontal competition between States, models and standards: a global struggle for law. And because of the impact that the regulation mechanism may have on the rule of law, one can see that what is actually at stake are the fundamental freedoms. The question remains: which of the libertarian, the procedural co-regulatory and the authoritarian co-regulatory model will surpass the others?

List of References

Ahlert, C., Marsden, C., Yung, C. 2004. 'How Liberty Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-regulation' *available online at* http://pcmlp.socleg.ox.ac.uk/text/liberty.pdf (last visited April 7, 2007).

Berman, P.S. 2002. 'The Globalization of Jurisdiction', *Univeristy of Pensylvannia Law Review* 151: 311-546.

Berns, T., Docquir, P.-F., Frydman, B., Hennebel, L., Lewkowicz, G. 2007. *Responsabilités des entreprises et corégulation*. Bruxelles: Bruylant, Series 'Penser le Droit'.

Birnhack, M.D. and Elkin-Koren, N. 2003. 'The Invisible Handshake: The Re-emergence of the State in the Digital Environment', *Virginia Journal of Law and Technology* 8: 6 *available online at* http://www.vjolt.net/vol8/issue2/v8i2_a06-Birnhack-Elkin-Koren.pdf (last visited April 7, 2007).

Boyle, J. 1997. 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors', *University of Cincinnati Law Review* 66: 177-205.

Chen, C. 2004. 'United States and European Union Approached to Internet Jurisdiction and Their Impact on E-commerce', *University of Pennsylvania Law Review* 25: 423-54.

Cheung, A.S.Y. 2006. 'The Business of Governance: China's Legislation on Content Regulation in Cyberspace', *New York University Journal of International Law and Politics* 38: 1-37.

Cowhig, David 2000. 'New Net Rules Not a Nuisance?', *Chinaonline News* (December 5).

Cullen, R. and Choy, D.W. 2005. 'China's Media: The Impact of the Internet', *San Diego International Law Journal* 6: 323-40.

Frydman, B. and Rorive, I. 2002a. 'Fighting Nazi and Anti-Semitic Material on the Internet: the Yahoo! Case and its Global Implications', Paper Presented on February 11, 2002 at the Cardozo School of Law during the Conference: "Hate and Terrorist Speech on the Internet: The Global Implications of the Yahoo! Ruling in France" *available online at* http://pcmlp.socleg.ox.ac.uk/YahooConference/ (last visited April 7, 2007).

Frydman, B. and Rorive, I. 2002b. 'Regulating Internet Content through Intermediaries in Europe and the USA', *Zeitschrift für Rechtssoziologie* 23: 41-59.

Frydman, B. 1997. 'Quel Droit pour l'Internet' in *Internet sous le Regard du Droit. Actes du Dolloque du 30 octobre 1997*. Bruxelles: Editions du Jeune Barreau de Bruxelles, pp.279-316.

Frydman, B. 2004. 'Coregulation: A Possible Legal Model for Global Governance', in De Schutter, B. (ed.) 2004. *About Globalisation. Views on the trajectory of mondialisation*. Brussels: VUB Brussels University Press, pp. 227-42.

Geist, M. 2001. 'Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP' *available online at* http://aix1.uottawa.ca/~geist/geistudrp.pdf (last visited April 7, 2007).

Geist, M. 2002. 'Fundamentally Fair.com? An Update on Bias Allegations and the ICANN UDRP' a*vailable online at* http://aix1.uottawa.ca/~geist/fairupdate.pdf. (last visited April 7, 2007).

Hans-Bredow-Institut 2006. *Final Report. Study on Co-regulation Measures in the Media Sector* (June) *available online at* http://www.hans-bredow-institut.de/forschung/recht/co-reg/Co-Reg-Draft_Final_Report.pdf (last visited April 7, 2007).

Hedley, S. 2006. *The Law of Electronic Commerce and the Internet in the UK and Ireland*. London: Routledge Cavendish.

Heffernan, J. 2006. 'An American in Beijing: An Attorney's Ethical Considerations Abroad with a Client Doing Business with a Repressive Government', *Georgetown Journal of Legal Ethics* 19: 721-31.

Hennebel, L. and Lewkowicz, G. 2007. 'Corégulation et Responsabilité Sociale des Enterprises', in Berns *et al*., pp. 147-226.

Katsh, E. 2006. 'Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace', *Lex Electronica* 10 *available online at* http://www.lex-electronica.org/articles/v10-3/katsh.pdf (last visited April 7, 2007).

Kerr, I. R. and Gilbert, D. 2004. 'The Role of ISPs in the Investigation of Cybercrime' in Mendina,T. and Brtiz, J. (eds) 2004. *Information ethics in an electronic age: current issues in Africa and the world*, Jefferson : McFarland Press, pp. 163-172.

Kesan, J.P. and Gallo, A.A. 2006. 'Why are the United States and the European Union Failing to Regulate the Internet Efficiently? Going Beyond the Bottom-Up and Top-Down Alternatives', *European Journal of Law and Economics* 21: 237-66.

Kreimer, S.F. 2006. 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link', *University of Pennsylvania Law Review* 155: 11-101.

Lacharite, J. 2002. 'Electronic Decentralisation in China: A Critical Analysis of Internet Filtering Policies in the People's Republic of China', *Australian Journal of Political Science* 37: 333-41.

Lee, C.-C. 2003. 'The Global and the National of the Chinese Media: Discourse, Market, Technology, and Ideology', in Lee, C.-C. (ed.) 2003. *Chinese Media, Global Contexts*. London: Routledge, pp.1-31.

Lichtman, D. and Posner, E. 2004. 'Holding Internet Service Providers Accountable', *Supreme Court Economic Review* 14: 221-60.

Lievens, E., Dumortier, J. Ryan, P.S. 2006. 'The Co-Protection of Minors in New Media: a European Approach to Co-Regulation', *U.C. Davis Journal of Juvenile Law & Policy* 10: 97-151.

Link, P. 2002. 'China: The Anaconda in the Chandelier', *New York Review of Books* (Apr. 11) *available online at* https://www.nybooks.com/articles/15258 (last visited April 7, 2007).

Manekshaw, C.S.J. 2005. 'Liability of ISPS: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act', *Computer Law Review and Technology Journal* 10: 1001-33.

Marzouki, M. 2006. 'The 'Guarantee Rights' for Realizing the Rule of Law', in Jørgensen, R.F. (ed.) 2003. *Human Rights in the Global Information Society*, Cambridge: MIT Press, Series 'The

Information Revolution & Global Politics', pp. 197-218.

McGeary, A. 2001. 'China's Great Balancing Act: Maximizing the Internet's Benefits while Limiting its Detriments', *International Lawyer* 35: 219-230.

Montero, E., Demoulin, M., Lazaro, C. 2004. 'La Loi du 11 mars 2003 sur les Services de la Société de l'Information', *Journal des Tribunaux* 6125: 81-95.

Newbold, J. 2003. 'Aiding the Enemy: Imposing Liability on U.S. Corporations Selling China Internet Tools to Restrict Human Rights', *University of Illinois Journal of Law, Technology and Policy* 2003: 503-29.

Nguyen, X. 2004. 'Collateralizing Privacy', *Tulane Law Review* 78: 553-604.

Palfrey, J.G. and Rogoyski, R. 2006. 'The Move to the Middle: the Enduring Threat of "Harmful" speech to the end-to-end principle', *Washington University Journal of Law and Policy* 21: 31-66.

Palzer, C. 2003. 'Co-regulation of the media in Europe. European provisions for the establishment of co-regulation frameworks', *Media, Law & Policy* 13: 7-27.

Poullet, Y. 2004. 'Technologies de l'Information et de la Communication et "Coregulation": une Nouvelle Approche?' in *Liber Amicorum Michel Coipel*. Bruxelles: Kluwer, pp. 167-88.

Price, M.E. and Verhulst, S.G. 2005. *Self-Regulation and the Internet*. The Hague: Kluwer Law International.

Qiu, J.L. 2000. 'Virtual Censorship in China: Keeping the Gate between the Cyberspaces', *International Journal of Communications Law and Policy* 4: 1-25.

Reed, K.M. 2000. 'From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce', *The Transnational Lawyer* 13: 451-76.

Rightswatch 2003. *White Paper. A way forward for notice and takedown* (July 4), *available online at* http://www.rightswatch.com/White_Paper_20030704_v1_FINAL.pdf (last visited April 7, 2007).

Rustad, M.L. and Koening, T.H. 2005. 'Rebooting Cybertort Law', *Washington Law Review* 80: 335-476.

Schiavetta, S. 2004. 'The Relationship Between e-ADR and Article 6 of the European Convention of Human Rights pursuant to the Case Law of the European Court of Human Rights', *The Journal of Information, Law and Technology* 2004, *available online at* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_1/schiavetta (last visited October 10, 2007).

Schultz, W. and Held, T. 2004. *Regulated Self-Regulation as a Form of Modern Government: An Analysis of Case Studies from Media and Telecommunications Law*. Eastleigh: University of Luton Press.

Schultz, T. 2005. *Réguler le Commerce Electronique par la Résolution des Litiges en Ligne. Une Approche Critique*. Bruxelles/Paris: Bruylant/LGDJ.

Sédaillian, V. 2005. 'Responsabilité des Prestataires Techniques: Le Droit Français', *Lex Electronica* 10 *available online at* http://www.lex-electronica.org/articles/v10-1/sedallian.pdf (last visited April 7, 2007).

Senden, L. 2003. 'Soft-Law, Self-Regulation and Co-Regulation in European law: Where Do They Meet?', *Electronic Journal of Comparative Law* 9 *available online at* http://www.ejcl.org/91/art91-3.html (last visited April 7, 2007).

Nas, S. 2004. 'The Multatuli Project. ISP Notice and Takedown' *available at* http://www.bof.nl/docs/researchpaperSANE.pdf (last visited April 7, 2007).

Strowel, A., Ide, N., Verhoestraete, F. 2001. 'La Directive du 8 juin 2000 sur le Commerce Electronique: Un Cadre Juridique pour l'Internet', *Journal des Tribunaux* 6000: 133-45.

Svantesson, D.J.B. 2005. 'The Characteristics Making Internet Communication Challenge Traditional Models of Regulation – What Every International Jurist Should Know About the Internet', *International Journal of Law and Information Technology* 13: 39-69.

Verdure, C. 2005. 'Les Hébergeurs de Sites Web: Victimes ou Régulateurs de la Société de l'Information?', *Droit de la consommation/Consumentenrecht* 68: 31-52.

Wahlquist, J. 2005. 'The World Summit on the Information Society: Making the Case for Private Industry Filtering to Control Extraterritorial Jurisdiction and Transnational Internet Censorship Conflicts', *International Law & Management Review* 1: 283-310.

Wanamaker, A. 2006. 'Censors in Cyberspace: Can Congress Protect Children From Internet Pornography Despite Ashcroft v. ACLU?', *Saint Louis University Law Journal* 50: 957-94.

Zittrain, J. 2003. 'Internet Points of Control', *Boston College Law Review* 44: 653-88.

Zittrain, J. 2006. 'A History of Online Gatekeeping', *Harvard Journal of Law and Technology* 19: 253-98.