Regulating Internet Content through Intermediaries in Europe and the USA

Zeitschrift für Rechtssoziologie
(revue de l'Institut Max Planck de Cologne),
2002, vol. 23 (1), p. 41-59

Benoît Frydman and Isabelle Rorive

Date de mise en ligne :15 mars 2003

Regulating Internet Content through Intermediaries in Europe and the USA

Benoît Frydman and Isabelle Rorive[1]

Summary: *This paper emphasises the key role played by Internet Service Providers (ISPs) in the current developments in Internet content regulation. At present, no common international standards govern free speech limits on the Internet. Racist speech constitutes the most controversial issue between Europe and the US. The enforcement of domestic law online has recently led to surprising court rulings in several European countries, putting transatlantic ISPs under pressure. The paper provides a detailed account of three of these cases: the early German Compuserve case, the famous French Yahoo! case and most recently the French J'accuse! case. Both European and American legislators have endeavoured to provide ISPs with "safe havens" (limitations of liability) and tentative procedural solutions like "notice and take down". These new regimes and their likely effects on ISPs are presented and discussed. It is suggested that, despite the lack of common standards, the combination of the American and the European provisions would strongly incite transatlantic ISPs to take down racist material. This, however, also risks affecting other controversial data, otherwise subject to free speech protection. The danger of a massive scheme for private censorship is compelling.*

1 Limits of free speech and the role of ISPs

1.1 Freedom of speech deserves constitutional protection in all modern democracies. However, the legal limits of free speech are not the same on both sides of the Atlantic. *Racist speech* constitutes the most striking and the most controversial example. It is tolerated in the US where it takes advantage of the shelter provided by the First Amendment of the Constitution[2]. On the contrary, it is banned in most European countries where it is a criminal offence and is prosecuted as such.

Not only history but also political philosophy account for this divergence. US constitutional law regards racist speech as a variety – however disgusting, dangerous and extremist – of political opinion and denies both the States and the Federal bodies the power to interfere with such kind of public debate. This regime is based upon the libertarian philosophy of government non-interference with individual liberty[3]. It has been established during the past forty years while the Supreme Court has largely eradicated most forms of public censorship[4].

The European approach, stated in article 10 of the Convention for the protection of human rights and fundamental freedoms, is fairly different. The European Court has persistently emphasised freedom of expression as one of the essential foundations of a democratic society and as one of the basic conditions for its progress and for "each individual's self-fulfilment". It is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society".[5] Nonetheless, freedom of speech is not absolute in Europe. It is a

1 We would like to warmly thank Dr. Christian Sandvig, Markle Fellow at the Program in Comparative Media Law & Policy, for his thorough and constructive comments on this paper and for having accepted the fastidious task of helping us with our English writing. It goes without saying that we take full responsibility for the content of this paper.

2 The First Amendment of the US Constitution reads as follows: "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*".

3 J. M. BALKIN, "The American System of Censorship and Free Expression", *in* I. Peleg (ed.), *Patterns of Censorship Around the World* (Chicago – Oxford: Westview Press, 1993) 155-172, esp. 157.

4 In 1964, the Warren Court ruling in *New York Times Co.* v. *Sullivan* (376 U.S. 254 (1964)), which protects the press from seditious libel claims by public officials, might be considered as a suitable landmark.

5 Recent decisions include E.C.H.R., *Tammer* v. *Estonia*, 6 February 2001, § 59 ; E.C.H.R., *Jerusalem* v. *Austria* 27 February 2001, § 32; E.C.H.R., *Thoma* v. *Luxembourg*, 29 March 2001, § 44; *Maronek* v. *Slovakia*, 19 April 2001, § 5; E.C.H.R., *Feldek* v. *Slovakia*, 12 July 2001,

qualified right, that "carries with it duties and responsibilities" and "may be subject to formalities, conditions, restrictions or penalties".[6] This narrower conception is shared by most of the other democratic countries, including Australia, Canada and Japan.

Restrictions and penalties mentioned in article 10 apply to racist speeches and some other questionable speeches that threaten, deny or even lead to the destruction of human dignity and integrity. They are proscribed in many European countries and are given no protection whatsoever by the European Council's institutions.[7] Moreover, in the E.U. itself, racist speech is likely to be entirely outlawed in the near future. Last November, the European Commission issued a proposal that would provide that the same racist and xenophobic conduct be unlawful in all Member States. It establishes the minimum approximation necessary to ensure that national legislation is sufficiently comprehensive and that effective judicial cooperation can be developed. The offences covered by the proposal include public incitement to violence or hatred for racist or xenophobic reasons and the dissemination of racist material by any means, including the Internet.[8]

1.2 As expected, both Europe and the US tend to apply their own free speech standards to Internet communications. Nevertheless, attempts to agree on common standards have made some progress lately [Mayer, this issue]. The Convention on Cyber-crime, adopted by the Council of Europe and opened to signature since the 23rd of November 2001, has already been signed by a large number of Member States[9], along with the United States of America, Canada, South Africa and Japan, all of whom participated actively in the negotiations.[10] With respect to content-related offences, the Convention fosters international prosecution of child pornography[11] and copyright infringements[12]. It does not extend to hate speech and incitement to violence. This is due to pressure from the US delegation who made clear that such a regulation of expression is contrary to the First Amendment of their Constitution and would prevent the US from signing the treaty.[13] As a compromise, the Council of Europe decided to make the hate-speech provisions the subject of an independent protocol that should be ready by mid 2002. Aside from defining and criminalizing the dissemination of racist propaganda and abusive storage of hateful messages, this instrument is expected to fight "unlawful hosting", i.e., hosting that aims to circumvent the laws of less permissive states.[14]

§ 7; E.C.H.R., *Ekin Association* v. *France*, 17 July 2001, § 56; E.C.H.R., *Sener* v. *Turkey,* 18 July 2000, § 39; E.C.H.R., *Perna* v. *Italy*, 25 July 2001, § 1.

6 Article 10 of the European Convention for the protection of human rights and fundamental freedoms. The entire provision reads as follows:
"*1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

7 See article 17 of the European Convention for the protection of human rights and fundamental freedoms: "*Nothing in this Convention maybe interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent that is provided for in the Convention.*"

8 Proposal for a Council Framework Decision on combating racism and xenophobia (Brussels, November 28, 2001, COM(2001) 664 final) <http://europa.eu.int/eur-lex/en/com/pdf/2001/com2001_0664en01.pdf> (last visited on January 25, 2002).

9 On November 23, 2001, 26 Member States out of 43 signed the Treaty <http://www. computer-world.com/storyba/0,4125,NAV47_STO66012,00.html> (last visited on January 25, 2002).

10 The Convention on Cyber-crime (Budapest, 23 November 2001) is available on the site of the Council of Europe at <http://conventions.coe.int/Treaty/EN/projets/FinalCyber crime.htm> (last visited on January 25, 2002).

11 Convention on Cyber-crime (Council of Europe), article 9.

12 Convention on Cyber-crime (Council of Europe), article 10.

13 Due to the extensive scope it traditionally assigns to the First Amendment, the US traditionally has resisted Treaties that would restrict its citizen's free speech rights. See, for instance, reservation 1 to the article 20 of the U.N.'s International Covenant on civil and political rights which provides that: "*Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.*"

14 See I. TALLO, "Racism and xenophobia in cyberspace", Report of the Committee on Legal Affairs and Human Rights, Council of Europe, Doc. 9263, 12 October 2001 <http://www.steptoe.com/webdoc.nsf/Files/184b/$file/184b.htm> (last visited on January 25, 2002). The second public version of the *Draft of the First Additional Protocol to the Convention on cybercrime concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems* was released on March 26, 2002. It is available at <http://www.legal .coe.int/economiccrime/cybercrime/AP_Protocol(2002)5E.pdf> (last visited on March 27, 2002).

Therefore, while Europe is giving itself efficient instruments to ban racist speech altogether, this kind of expression remains entirely legal in the US.[15]

1.3 One question then arises: why are the Internet service providers (ISPs) involved in such a debate? At first glance, the uncertain limits of free speech do not concern them. Nevertheless, recent court cases show the great extent to which they are embroiled in these issues.

Cyberspace is a global forum where national territory is of little relevance. "As far as the Internet is concerned, not only is there perhaps 'no there there', the 'there' is everywhere where there is Internet access."[16] When one logs on to a Website, one does not really pay attention to the location of the site. Most of the time, the user does not even know where it is hosted. What does really matter for the Internet surfer is to find the information he or she is looking for.

The perspective of a government is quite different. Since its jurisdiction is confined to a national territory, it cannot efficiently control Websites and other data posted on the Internet from outside its borders. Consider a German prosecutor who would take legal action against an unlawful racist message, accessible from any computer in Germany provided with a network connection. Assume that this message was posted by an American citizen on a Website hosted in the US. In such a case, the prosecution is most probably doomed to failure because German prosecutors lack jurisdiction in the US. Moreover, the questionable content is there under the protection of the First Amendment of the Constitution.

1.4 While going after the content provider is not always possible, a more successful strategy is to put pressure on the ISPs in charge of the communication process. A public authority can issue injunctions to national access providers or even to large foreign hosting providers as soon as they have business interests or a subsidiary operating in Europe. It is therefore tempting for governments to try to recover some control over the Internet at the expense of the ISPs. On the other hand, most of the governments want to stimulate the growth of the "information society" and e-business. They are not ready to impose too many burdens on the ISPs. But, in Europe, they count on the ISPs to play their part in "co-regulation" of the Internet, which implies an original mixture between self-regulation and government intervention.

On the whole, the ISPs are far from being pleased to play such a role. Controlling the content of the messages they host or give access puts them in an uncomfortable position. The access providers in particular argue that they should be treated as a "common carrier" of goods or as telephone carriers. These are usually not asked to check the content of the goods transported or the conversations held through their networks.

1.5 The current situation has created a great uncertainty. Legal proceedings have been launched and have led to interesting and sometimes surprising judicial rulings. Both in the US and in the European Union, parliaments have responded to the problem.

This paper aims at weighing the ISPs' duties against the liabilities they are subject to. We shall first examine recent cases that have involved major ISPs in Europe. Then, we shall review the legislative rules set up both by the US Congress and by the institutions of the European Union. Finally, we will consider the effects these new rules might have. In other words, which attitude are transatlantic ISPs likely to adopt towards questionable content in the next few years?

2 US ISPs facing European court injunctions: three topical cases

2.1 In recent years, some major ISPs like *CompuServe*, *Yahoo* and *America On-Line*, faced civil or criminal proceedings related to questionable content, especially pornographic or racist materials they hosted or gave access to.

2.2 The first major case arose in Germany and affected the German subsidiary of *CompuServe*, in particular its managing director, Mr. Somm. The facts were as follows. The US company *CompuServe Inc.* hosted

15 See also Committee to Study Global Networks and Local Values, Computer Science and Telecommunications Board, National Research Council (US), *Global Networks and Local Values. A Comparative Look at Germany and the United States*. Washington DC, National Academy Press 2001, chapter 5.

16 *Blumenthal v. Drudge and AOL, Inc.* 992 F. Supp. 44 (D.C.C. April 22, 1998), 1998 U.S. Dist. LEXIS 5606 (p. 5), paraphrasing Gertrude Stein.

newsgroups of a paedophile nature on its news server. Its 100% German subsidiary, *CompuServe GmbH*, allowed German subscribers to access these newsgroups at a local dial up rate by providing them with dial-in nodes and telecommunication lines. However, there were no contractual relationships between *CompuServe GmbH* and the customers. The American company was the only one to have such relations with the German subscribers. As we shall see, the German authorities chose not to prosecute *CompuServe Inc*. and its directors in the US.

Following a search, the investigating German police officers selected five pornographic newsgroups involving children as examples for the existence of newsgroups whose names unequivocally designated child pornography to the personal notice of Mr. Somm. As his company did not have the technical ability to cut off access to the newsgroups, Mr. Somm forwarded the list to *CompuServe Inc.* with a request to remove the newsgroups at stake. The American company blocked said newsgroups. Then, the German police handed over to Mr. Somm a list indicating 282 accessible newsgroups providing violent, child, or animal pornography representations which were accessible for the customers of *CompuServe Inc.* in Germany. Again, Mr. Somm passed on the list to the parent company and requested blocking or deletion. For two months, *CompuServe Inc.* blocked the majority of the newsgroups on the list. Afterwards, the company and Mr. Somm stated in electronically accessible letters that they did not feel obliged to intervene further since *CompuServe* now provides a control tool called '*Cyber Patrol – Parental Control'* free of charge. This control software, which was also available in a German language version, enabled subscribers to block themselves the access to whatever newsgroups they chose.

This did not satisfy the German prosecutor since the safeguard program did not block public access to hard pornography and paedophilia. Mr. Somm was accused of facilitating access to violent, child, or animal pornographic content stored in explicitly named newsgroups for hard pornography and participating in a criminal offence (i.e., negligent violation of the German Act on the Dissemination of Publications Morally Harmful to Youth). In the end of the pleadings, the state prosecutor petitioned the court to acquit the Defendant because on the facts of the case, he could not be held criminally liable. Nonetheless, on the 15th of July 1998, the *Amtsgericht München* convicted Mr. Somm to two years suspended prison sentence, three years' probation and fined him 100,000 marks for the distribution of child pornography and other illegal materials.

In 1999, the *Landgericht München* reversed this ruling and acquitted Mr. Somm. The appeal Court gave him the benefit of the exemption of liability provided by par. 5 (3) of the 1997 German *Teleservices Act (TDG)*. The Court decided that the manager was not at fault because he was not technically able to remove the newsgroups and because he made all reasonable efforts to transmit the request to the parent company.[17]

2.3 The next dramatic case involved *Yahoo! Inc.*. Decided in May 2000 by Parisian judge Jean-Jacques Gomez, it has led to both concern and interest in the US.

Contrary to the *Compuserve* case, the matter here was addressed in a civil trial[18] and the US parent company was directly involved.[19] Two French Non-Governmental Organisations (NGOs) fighting against racism and anti-Semitism complained that *Yahoo! Inc.* was allowing the sale of thousands of pieces of Nazi memorabilia through its online auction service[20], while in France[21] the sale of Nazi-related items is regarded as a criminal offence. The auction site was hosted in the US but could of course be accessed from France. *Yahoo! Inc.* was also blamed for hosting several anti-Semitic pages on *Geocities*[22], where one could find, inter alia, *Mein Kampf* and *The Protocols of the Elders of Zion*.

Under the threat of a 100.000 FRF daily penalty (~ 16.000 Euro), the Court ordered *Yahoo! Inc.* to take all appropriate measures in order to prevent French Internet surfers or people located on the French territory

17 Prof. Dr. ULRICH SIEBER, Dr. HANS-WERNER MORITZ and WOLFANG DINGFELDER (Defense Lawyers), "Acquittal of Mr. Felix Somm by the Langericht München (Regional Court of Munich)", *Digital Law Net*, November 17, 1999. See also "Comments of Dr. HANS-WERNER MORITZ (Defending Counsel) on the Written Grounds for the Judgment of the Local Court", *Digital Law Net – Papers*; G. BENDER, "Bavaria v. Felix Somm: The Pornography Conviction of the Former CompuServe manager", *International Journal of Communications and Policy*, January 14, 1998.

18 The action was based on article 809 NCPC ("Nouveau Code de procédure civile") which states that the Judge of emergency proceedings has the power to put an end to a patent infringement of the law ("*trouble manifestement illicite*").

19 Note that *Yahoo France* was sued for providing a link and access to the prohibited content through the Yahoo.com Website. To some extent, it complied with the Judge's order to issue to all Internet surfers a warning informing them of the risks involved in continuing to view the pro-racist sites.

20 <http://auctions.yahoo.com>. An example of the controversial auction page may be found at <http://www.legalis.net/jnet/illustration/yahoo_auctions.htm> (last visited on January 25, 2002).

21 See article R. 645-1 of the French Criminal Code that prohibits the wearing and display in public of Nazi uniform or symbol, except in the context of historic presentation.

22 <http://www.geocities.com>.

from accessing auction sales of Nazi items, and more broadly from accessing any other site or service that promotes Nazism or denies Nazi crimes.[23] In addition to challenging the French court's jurisdiction and calling upon the First Amendment protection, *Yahoo! Inc.* objected that it was technically not feasible to put such measures into place because it was impossible to trace the users' nationality. And, even if such measures were possible, the high implementation cost would put the company at risk.

In November 2000, Judge Gomez took an additional decision based on a report by international experts.[24] These experts considered that "nearly 70% of IP addresses allocated to French surfers can be linked with certainty and be filtered." For the other 30%, they were of opinion that a "declaration upon honour of his nationality by the user" could achieve a significant filtering success rate. The Judge gave three months to *Yahoo! Inc.* to implement such measures.

These French decisions did not remain without consequences. Under pressure from US lobbies, *Yahoo! Inc.* banned hate-related goods (Nazi and KKK items in particular) from its auction site and removed numerous pro-Nazi WebPages from *Geocities*.[25] At the same time, *Yahoo! Inc.* started charging users to post items on the auction site.[26] The company said that the decision to remove the controversial goods had nothing to do with the French judge's injunction, however.

Concurrently, *Yahoo! Inc.* filed a counter-suit in a federal dictrict court, San José, California, requesting that the French decisions be declared void under the First Amendment of the US Constitution. The company also contested the French rulings on two grounds: first, that it is technically impossible to block access using filtering systems and second, that the French court has overstepped its jurisdiction, in other words that it should not be able to impose its national laws on a US company.

In November 2001, the US District Court issued the declaration *Yahoo! Inc.* was looking for, i.e., that the First Amendment of the Constitution that embodies the right to free speech precludes enforcement within the US of the French ruling.[27] The two French NGOs that launched the proceedings in France have appealed this decision and contended that *Yahoo! Inc*. should not be shielded from French law by the First Amendment. They are unlikely to succeed because of the legal principles that prohibit the enforcement of foreign judgments when the latter are contrary to the public policy of the forum.[28]

Other actions brought against *Yahoo! Inc.* in various European countries did not lead to the same result as the French rulings, either. In March 2001, a German court announced that it would not prosecute the company in relation to the Internet auction of Nazi items, otherwise illegal to sell conventionally, because the online portal is not liable for the legality of items posted for sale on its Websites. While Germany has some of the strongest laws against hate literature in the world, the German court reportedly recognised *Yahoo! Inc.* as an ISP and, as such, ruled that the company should not be held liable for the content of its auction Websites.[29]

2.4 As one could expect, the *Yahoo!* ruling caused human rights activists to take further action before the French Judiciary. *J'accuse!* (an association aimed at eradicating racism on the Internet and named after Zola's famous paper in the *Dreyfus case*) filed a case[30] against the majority of the French Internet access providers as well as the French ISP industry group, the *AFA*[31]. These ISPs, amongst whom one can find the French subsidiary of *AOL*, were charged with allowing French Internet users to access a US-based portal called *Front 14.org*, which hosts Nazi and other racist sites on its server at no charge. The ISPs claimed that they should not be responsible for monitoring their users' behaviour arguing that they are "only carriers" and

23 See the *Ordonnance de référé du Tribunal de grande instance de Paris*, May 22, 2000 at http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm (last visited on January 25, 2002).

24 For a summary of the report of the international experts, go to <http://www.juriscom. net/txt/jurisfr/cti/tgiparis20001106-rp.htm#texte> (last visited on January 25, 2002). For the report in full, go to <http://www.legalis.net> (last visited on January 25, 2002).

25 *Yahoo ! Inc.*'s new policy with respect to hate material took effect on January 10, 2001.

26 According to *Yahoo! Inc.* as long as the auction service was free of charge, it was protected by the freedom of expression principle. See E. LAUNET, "Objets nazis: Yahoo persiste. Action juridique du portail aux Etats-Unis", *Libération.com*, June 9 & 10, 2001.

27 *Yahoo! Inc.* v. *La ligue contre le racisme et l'antisémitisme* 2001 U.S. Dist. North. Dist. California (San Jose Div.), Case No C-0021275 JF, November 7, 2001 <http://www.cdt.org/ speech/>; <http://www.juriscom.net/en/txt/jurisus/ic/dccalifornia20011107.htm> (last visited on January 25, 2002).

28 On this point, see the arguments put forward in the Application of *Amici Curiae* for Leave to File Brief in Support of Yahoo! Inc.'s Motion for Summary Judgment, esp. 13-21 <http://www.cdt.org/speech/> (last visited on January 25, 2002).

29 See J. LYMAN, "German Court Rules Yahoo! Not Liable For Nazi Auctions", *NewsFactor Network,* March 28, 2001.

30 See the *Assignation en référé* brought by *J'accuse!…- action internationale pour la justice* available at <http://www.chez.com/aipj/assignation1.htm> (last visited on January 25, 2002).

31 The AFA stands for "*Association des Fournisseurs d'accès et de Services Internet*".

that they "cannot become the police". "Controlling or limiting citizens' access to the Internet is a prerogative which only belongs to public authorities", they said.[32] The ISPs also claimed that their efforts to develop self-filtering techniques were sufficient.

Jean-Jacques Gomez, the same Judge that presided in the *Yahoo!* case, handled the proceedings in a very unusual way. At the end of the first pleadings, he decided to reopen the debates and asked the parties to choose what he called "great witnesses", "in order to deepen and broaden the discussion on all factual, ethical and technical sides". Debates in the courtroom took place during two days[33] – unusual in the French judicial process and completely unheard of in the course of emergency proceedings. On the 30th of October 2001, the Judge held that the racist portal violates not only the French law but also the European Convention for the protection of human rights and fundamental freedoms together with the Universal Declaration of human rights.[34] The ruling gave ten day notice to the hosting provider of *Front14.org*, the US company SkyNetWeb Ltd (which refused to take part in the proceedings), to say what measures it intends to take to rectify the situation.

However, Gomez seemed reluctant to go one step further than in the *Yahoo!* case, especially regarding access providers. In his ruling, the Judge neither condemned the access providers nor issued formal injunction against them. He asked them to "*freely*" determine which measures they consider necessary and possible as to prevent Front14 from pursuing its illegal activity. He said that at present "there is no law under which access providers are compelled to filter the access on the Net". In fact, the French Parliament is currently discussing the *Information Society Act* that intends to give to the Judge of emergency proceedings (i.e, the *juge des référés*) the power to order all necessary measures to stop any breach of French law caused by online services. The New French Act on the Information Society (*Loi sur la société de l'information*) is likely to empower the judge dealing with emergency proceedings (*Président du tribunal de grande instance*) to order ISPs to take all appropriate measures which are necessary to cease an infringement caused by online services, including cutting access to them (new article 43-8-3 to be added to the 1986 *Freedom of Communication Act*).

In his opinion, judge Gomez nevertheless stressed the risks of the situation. He compared the Internet to a nuclear power plant working out of control in the centre of the city and asked for legislative intervention.

In Switzerland, the Front14 Nazi gateway was dealt with in a different way. The NGO *Aktion Kinder des Holocaust* managed to convince the federal police to put the gateway on the "black list" which is voluntarily blocked by Swiss ISPs. This seems to be the usual practice in Switzerland.[35]

Meanwhile *Front14.org* has disappeared from the Web altogether (at least, under this name), allegedly owing to an attack by hackers.[36]

3 Immunity and liability limitations of ISPs in US law

32 M.-J. GROS and E. LAUNET, "Quels verrous contre le 'portail de la haine'?", *Liberation – Multimédia,* June 14, 2000; C.B., "J'accuse!.. les fournisseurs d'accès", *Les News.net*, June 18, 2001.

33 At the request of the complainant, the following witnesses were heard, *inter alia*:
- three legal experts, according to whom filtering is technically feasible, but complex and never perfect;
- a popular philosopher, Alain Finkelkraut, who asked for a coming of the law on the Internet;
- the director of the weekly *Nouvel Observateur*, Laurent Joffrin, who criticized the access providers' defence. He said that neutrality is not acceptable when facing racism and compared their role to the trains that conveyed the Jews to the concentration camps during World War II;
- a Civil Servant from the Ministry of National Education;
- a professor at the renowned *Sorbonne*;
- a sociologist at the *Centre National pour la Recherche Scientifique* (which is the French national body supporting research).

The defence also called two "great witnesses" in the courtroom: Joel Boyer, the national secretary of the C.N.I.L. (*Commission nationale de l'informatique et des libertés*) and Meryem Marzouki, president of the I.R.I.S. network (*Initiative pour un réseau Internet solidaire*), who both emphasized the need to protect freedom of communication.

For press comments, see E. PANSU, "Le filtrage dans le prétoire", *Transfert*, September 4, 2001; E. LAUNET, "Filtrage de la toile: la justice convoque les 'grands témoins'", *Liberation – Quotidien*, September 5, 2001; E. LAUNET, "Querelles d'experts sur le filtrage de la Toile", *Liberation – Multimédia,* September 12, 2001.

34 *Ordonnance de référé du Tribunal de grande instance de Paris*, October 30, 2001 <http://www. chez.com/aipj/ordonnance30oct2001> (last visited on January 25, 2002).

35 See V. FINGAL, "Nazis pris dans la toile", March 27, 2001 <http://www.chez.com/aipj/ akdh1.htm> (last visited on January 25, 2002).

36 E. LAUNET and E. RICHARD, "Les imbroglios du portail de la haine", *Liberation – Multimédia,* November 8, 2001.

3.1 Even in the US, the ISPs have been challenged for unlawful content they were hosting or giving access to. In 1995, the Supreme Court of the State of New York laid down what has been since known as the *Stratton Oakmont* ruling.[37] It held the ISP *Prodigy Services Company* liable for an anonymous defamatory message posted on one of its bulletin boards called *Money Talk*, which at the time was the leading and most widely read financial computer bulletin board in the US. The message accused the two plaintiffs, a securities investment banking firm (*Stratton Oakmont, Inc*.) and its president of committing criminal and fraudulent acts in connection with a public stock offering. The Court held that *Prodigy* should be regarded as the publisher of the libel and not as a mere distributor because a paid employee monitored the bulletin boards. In the opinion of the court, this editorial control through an agent meant that *Prodigy* could not be considered as a mere "passive conduit". According to the court, *Prodigy* assumed an effective editorial control by its stated policy that it was a family oriented computer network.[38]

3.2 The extent to which ISPs were put in the frontline of judicial proceedings gave rise to great concern. The legislature of the United States of America and the parliament of the European Union decided to take the problem into their own hands. One of their aims was to avoid undesirable judicial rulings and legal uncertainty that could stand in the way of the "information society" and slow down "e-business". In the US, the legislature's position was so strong as to prevent any State or Federal regulation from interfering with the development of the Internet or from having a "chilling effect" on freedom of speech on the network.

3.3 In this context, the US Congress overruled the *Stratton Oakmont* ruling without any delay. In the *Communication Decency Act (CDA)* of 1996, the ISPs were sheltered from detrimental torts. Section 230 (c) (1) of this Act immunises providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others. The ISPs are therefore exempt from any editorial liability for content they host or give access to:
"No provider or user of an interactive computer service shall be treated as publisher or speaker of any information provided by another content provider".[39]

If not overturned, the *Stratton Oakmont* decision would have certainly discouraged the ISPs from managing the material they were hosting. By implementing a content policy, they would have exposed themselves to the strict liability standards normally applied to original publishers of defamatory statements. An important purpose of section 230 was therefore to remove the disincentives to self-regulation created by this ruling.[40] With this provision, lawsuits seeking to hold an ISP liable for its exercise of a publisher's traditional editorial function are barred.

3.4 In line with the legislative intent, the US courts have applied the immunity provision in an extensive manner[41]. For instance, they ruled that the hosting provider would not be held liable even if it was aware of the unlawful character of the hosted content; even if it had been notified of this fact by a third party who was harmed by the illegal content[42], and even if it had paid for the illegal data[43].

37 *Stratton Oakmont, Inc.* v. *Prodigy Services Company*, 1995 N.Y. Misc. LEXIS 229, 1995 (N.Y. Sup. Ct., May 24, 1995).

38 The court stressed this fact as to distinguish the case at hand with the *Cubby* case where the ISP *Compuserve* was held not liable for defamatory statements carried by one of its forums since it had "little or no editorial control" (*Cubby, Inc.* v. *Compuserve, Inc.* 776 F. Supp. 135 (S.D. N.Y. 1991)). On this point, the court went on stating that "The key distinction between Compuserve and Prodigy is two-fold. First, Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards. Second, Prodigy implemented this control through its automatic software screening program, and the Guidelines which Board Leaders are required to enforce."

39 CDA 47 U.S.C. § 230 (c) (1) <http://www4.law.cornell.edu/uscode/47/230.html> (last visited on January 25, 2002).

40 In the, same line, see section 230 (b) (4) that provides: "It is the policy of the United States to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material". In *Doe* v. *AOL, Inc.* (2001 Fla. LEXIS 449 (Fla, March 8, 2001)), the Supreme Court of Florida stated that "Congress's clear objective in passing section 230 of the CDA was to encourage the development of technologies, procedures and techniques by which objectionable material could be blocked or deleted either by the interactive computer service provider itself or by the families and schools receiving information via the Internet".

41 See B. HOLZNAGEL, "Responsibility for Harmful and Illegal Content as well as Free Speech on the Internet in the United States of America and Germany", *in* C. Engel and H. Keller (eds.), *Governance of Global Networks in the Light of Differing Local Values*, Baden-Baden, Nomos, 2000, p. 9-42, esp. 29-33.

42 As a defamatory case, see *Zeran* v. *AOL, Inc.* 958 F. Supp. 124 (D.C.); 129 F. 3d 327 (4th Cir. 1997), 1997 U.S. App. LEXIS 31791. As a case dealing with advertisement for child pornography, see *Doe* v. *AOL, Inc.*, 2001 Fla. LEXIS 449 (Fla, March 8, 2001).

43 As a defamatory case, see *Blumenthal* v. *Drudge and AOL, Inc.* 992 F. Supp. 44 (D.C.C. April 22, 1998), 1998 U.S. Dist. LEXIS 5606. In this case, the alleged defamatory statement was not anonymous but sent by a columnist with whom AOL contracted and paid a monthly fee.

However, the immunity of ISPs is not absolute. In the highly sensitive issue of child pornography, they are expected to cooperate with public authorities. The 1990 *Protection of Children from Sexual Predators Act* requires online service providers to report evidence of child pornography offences to law enforcement agencies. Otherwise, they face a civil fine of up to $50,000 in the first instance and $100,000 for any subsequent failure.[44]

Moreover, the *CDA* did not address copyright. This question of copyright was dealt with in the 1998 *Digital Millennium Copyright Act (DMCA)*.[45] The *DMCA*[46] adds a new section 512 to the 1976 *Copyright Act*, which limits the liability of online service providers for copyright infringements. This clause codifies the terms of an agreement (referred to as the *Washington agreement*), which was negotiated between copyright holders and online intermediaries. The *DMCA* is less favourable to the ISPs than the general immunity regime. It sets up cases of liability exemptions, which put new duties on ISPs. The hosting provider is exonerated from any direct or vicarious liability for copyright infringements whose content it is hosting providing that it meets three cumulative conditions[47]:

1. The host must have no knowledge that the hosted content is infringing or must not be aware of facts or circumstances from which infringing activity is patent;
2. If the provider has the right and ability to control the infringing activity, it must not receive a financial benefit directly attributable to the infringing activity;
3. And finally, upon receiving proper notification of claimed infringement, the host must "act expeditiously to remove or disable access to the material".[48]

With respect to this third condition, the statute implements the so-called *notice and take down procedure*. When a copyright holder discovers that his or her right has been infringed, he or she must formally notify the infraction to the ISP's designated agent. The ISP must then remove the material or disable access to it quickly, otherwise it could be liable for damages. It must also promptly notify the subscriber that it has removed or disabled access to the material. The subscriber may then dispute the validity of the notice and send a formal counter notification to the ISP. In that case, the ISP has to inform the complainer that it will *put back* the controversial data in 10 business days, unless the complainer filed an action against the content provider seeking a court injunction.

This procedural mechanism is ingenious because it opens the door to an amiable settlement of the conflict, without putting the ISP in the position of a judge who has to decide if the controversial data are infringing or not.

4 Liability limitations of ISP's in European law

4.1 In Europe, the matter was handled by the European Union in its Directive on e-commerce[49], which was due to be implemented by the Member States before the 17th of January 2002.[50] The European regime of liability limitations is much more balanced than the CDA immunity clause. It also leaves more room for state intervention, a position that is consistent with the European approach to freedom of speech as a qualified right. With respect to ISP liability, the European Directive was largely modelled upon the 1997 *German*

44 Section 42 U.S.C. § 13032. The *Protection of Children from Sexual Predators Act* amends 18 U.S.C. § 2702(b) of the 1986 *Electronic Communications Privacy Act* to create an exception to the general statutory bar against a public provider's voluntary disclosure of customer communications to third parties.

45 17 U.S.C. 512 (C) <http://www.loc.gov/copyright/legislation/hr2281.pdf> (last visited on January 25, 2002).

46 In particular, Title II of the DMCA, "Online Copyright Infringement Liability Limitation Act".

47 Section 512 (c) (1) (A) (B) (C): "Information Residing on Systems or Networks At Direction of Users". Section 512 (d) contains a similar provision with respect to hyperlinks, online directories, search engines and the like.
Note that the failure of a service provider to qualify for any of the limitations in section 512 does not necessarily make it liable for copyright infringement. The copyright owner must still demonstrate that the provider has infringed, and the provider may still avail itself of any of the defences, such as fair use, that are available to copyright defendants generally (Section 512 (l)).

48 See the description of this procedure in A. STROWEL and N. IDE, "Liability of Internet Intermediaries: Recent Developments and the Question of Hyperlinks", *Revue internationale du droit d'auteur*, July and October 2000, p. 56.

49 Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce", June 8, 2000), art. 12-15.

50 Note that articles 12 to 15 of the Directive on e-commerce have in any case "direct effects" because these provisions are sufficiently precise and unqualified so that Member States have to adopt a specified behaviour. This means that a Member State which has not passed national law on time is nevertheless bound by these provisions towards people under its jurisdiction. With respect to the e-commerce directive, see <http://www.droit-technologie.org/fr/1_2.asp?actu_id=506> (last visited on January 25, 2002).

Teleservices Act[51]. However, the European provisions put slightly more burden on the ISPs in comparison with the former German statute.[52]

Far from seeking to harmonise national laws by setting common standards of liability, the Directive primarily intends to set up "liability havens", i.e., cases where the ISPs are exempted from direct and vicarious liability both at the civil and at the criminal level.[53]

4.2 As a matter of principle, the Directive states in article 15, that the European Member States should neither impose a general obligation on the ISPs to monitor the information which they transmit or store, nor a general obligation to actively seek illegal activities on the network. But the Member States may compel the ISPs to promptly inform the public authorities about illegal data or infringements reported by recipients of their services. They may also oblige the ISPs to communicate information enabling the identification of their subscribers at the request of public authorities. Undoubtedly, the Directive seeks to stimulate co-regulation, i.e., some kind of collaboration between the ISPs and the public authorities.

In this line, the Directive explicitly mentions the possibility for national courts or administrative authorities to *enjoin* both the access providers and the hosting providers to prevent or to put an end to a breach of the national law in accordance with Member States' legal system (art. 12.3 and 14.3). In any case, the European service providers will have to block questionable data when asked to do so. In this respect, the administrative authority of European countries in general, and the police body in particular, are usually entitled to give such an injunction.

As regards to what the Directive calls "mere conduit", which covers *inter alias* access providing activities, article 12 states that the provider will not be *liable* for information transmitted on condition that he plays only a passive role. This implies that it

"*(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."

With respect to hosting activities in particular, article 14 of the Directive states that the provider will not be *liable* for the information stored providing that:

"(*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."

4.3 The regime set up by article 14 of the European Directive is rather similar to the one enforced by the US Congress in the 1998 *Digital Millennium Copyright Act*. However, while in the US the scope of the regime is strictly limited to copyright infringements, in Europe it applies to all breaches of the law, as, for instance, the legal consequences of defamation or of hate speech. Moreover, the US provision established a formal "notice and take down" procedure, while the European Directive does not specify the essential information that such a notification should include, leaving the matter to be settled by agreements between business operators through codes of conduct. Furthermore, no "put back procedure" is set up or even mentioned in the European Directive. Despite these important differences, the US *DMCA* and the European general provisions share a common spirit. While it appears difficult, if not impossible, to reach substantial common standards regarding content control on the Internet, it seems much easier to adopt common procedures that may lead to similar results or, at the very least to a cease-fire with the business operators.

51 Before being reformed on January 1, 2002 by article 1 of the *EGG*, par. 5 of the 1997 *Teleservices Act* (*TDG*) read as follows:
"*(1) Providers shall be responsible in accordance with general laws for their own content, which they make available for use.*
(2) Providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content.
(3) Providers shall not be responsible for any third-party content to which they only provide access. The automatic and temporary storage of third-party content due to user request shall be considered as providing access."

52 See the new par. 8-11 of the *TDG*.

53 Note that outside these "liability havens", this is the domestic law of the Members States which apply to decide whether the ISPs are liable or not (see A. STROWELS and N. IDE, *o. c.*, p. 64).

5 Likely effects of the new European rules on transatlantic Internet services

5.1 The "notice and take down" system is a good example of the *new model of governance that characterises globalisation*. It implies a double shift *from substantial to procedural regulation and from States' regulation to global co-regulation*. But even if this system shows that a bringing together of the US and Europe is achievable through the adoption of common procedures, it is far from being a panacea with respect to free speech. This system will probably stimulate and facilitate the removal of illegal content from the Internet. ISPs will be anxious to preserve the liability limitation provided by statute and therefore will act expeditiously when being notified of any infringement. It is also possible that in the long run the most important ISPs will avoid hosting or giving access to material that appears questionable, unorthodox or disturbing so as to secure their reputation in the market.

American ISP's acting in this way are backed by a CDA clause called "*the Good Samaritan provision"*, which 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."[54]

This may lead to politically correct or even economically correct unofficial standards that may constitute an informal but quite efficient mechanism for content-based private censorship. In this case, the First Amendment protection may be formally upheld while freedom of speech would no longer be effectively guaranteed.

Such an outcome is not simply speculative. The current situation is comparable to the regime of press control adopted in several European countries in the 19th century – for instance in the Netherlands, including Belgium from 1815 to 1830. This system was aimed at controlling the press while the Constitution formally guaranteed the freedom of expression and abolished censorship. Printers were required to pay a deposit as a kind of warranty in case they would be held liable for writings they had published. This was most effective for the Government in place because few printers dared to take any financial risk by publishing questionable material. This private censorship seems to have been even more severe than the previous regimes of government censors.

A similar situation could prevail on the Internet in the near future. The combination of the American "Good Samaritan provision"[55] and the European conditional exemptions of liability create a compelling incentive for ISPs to remove any controversial material whenever they are informed by an authority or even informally notified that a Website, a bulletin boards or a newsgroup they are hosting contain unlawful, infringing or otherwise controversial material.

5.2 This new legal environment will then probably produce two normatively opposite effects. On the one hand, it will provide public authorities and human rights activists with better tools to limit the influence of racist, Nazis, anti-Semitic and other kind of hate speeches on the Internet. On the other hand, this might be the slippery slope to indiscriminate private censorship.

The willingness to exploit these new tools is certainly clear in Germany where public authorities have recently taken new actions against racist and Nazi material hosted by American ISPs. In May 2001 and again in January 2002, the Federal Office for the Protection of the Constitution (Bundesamt für den Verfassungsschutz) has notified *Ebay Inc*., a California company which runs the world largest shopping Website, about the sale of Nazi-related songs, books, clothing and paraphernalia on its "marketplace". Each time, *Ebay* reacted to the notice and promptly disabled access to the controversial items. In addition, the company formally declared that it "will no longer host the sale of memorabilia from the Nazi period or anything related to fanatical groups."[56]

54 CDA 47 U.S.C. § 230 (c) (2) (A) <http://www4.law.cornell.edu/uscode/47/230.html> (last visited on January 25, 2002).

55 In addition, contractual provisions generally allow the hosting provider to freely remove or disable access to any material that appears controversial in one way or another.

56 Statement issued in May 2001, quoted by A. ROSENBAUM in "Nazi Items Gone From Ebay Under German Pressure", *Newsbytes* <http://www.newsbytes.com/news/02/ 173746.html> (last visited on January 25, 2002). When trying to buy a Nazi propaganda book or a World War II German army uniform, the user is now given the following notice: "Dear User: Unfortunately, access to this particular category or item has been blocked due to legal restrictions in your home country. Based on our discussions with concerned government agencies and Ebay community members, we have taken these steps to reduce the chance of inappropriate items being

The recent steps taken by J. Büssow, the President of the Government of the County (Regierungsbezirk) of Düsseldorf, are signs of the same tendency. Not only has he challenged US ISPs to help combat neo-Nazi propaganda on the Internet[57], but, under the threat of an up to 500,000 mark fine, he has also ordered access service providers established on its territory to block access to a number of Nazi and racist sites based in the US. Internet surfers logging on through these ISPs have been redirected to the government Website when trying to access the banned US sites. Such a firm attitude has not been unanimously welcomed within Germany. The measures implemented by J. Büssow have been criticised as akin to censorship.[58]

In the case of hate speech, the European regime of conditional liability exemption and the "notice and take down" procedure may work as an efficient tool to enforce the rule of international law on the Internet. Indeed, article 20-2 of the 1966 U.N.'s International Covenant of Civil and Political Rights prescribes that "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law". The US have made explicit reservation about this provision because of the First Amendment of its Constitution. But, as we have seen, American hosting providers are likely to obey this rule in order to benefit from the liability incentive provided by the European legislation. Hate speech could thus be banned to a large extent in the US regardless of the American Constitution.

5.3 The compelling incentive to censure created by the combination of the e-commerce Directive and the "Good Samaritan provision" will not only apply to items that promote racism, Nazism, paedophilia or other obviously illegal data. It will also affect other material, otherwise legitimate, that is controversial for any reason.

Under the current legal provisions, ISPs are strongly encouraged to quickly remove any material when notified, even informally, by any third party that these data are infringing, defamatory, dangerous, seditious, inaccurate or otherwise illegal or damaging. This situation generates an obvious "chilling effect" on freedom of speech on the Internet, which is not consistent with the protection guaranteed by Article 10 of the European Convention on human rights.

The European regime concerning ISP liability should then be amended by law or supplemented by self-regulation in order to avoid this institutionalisation of massive private censorship. In particular, the "notice and take down" procedure should be improved in a way that could better protect the rights of the content provider. The procedure should be at least counterbalanced by a "notice and put back procedure" (such as in the *DMCA*) that will relieve the ISPs of the decision to remove the controversial data and give it back to the parties themselves or to a judge, if they fail to reach an agreement.

6 Conclusion

The heroic idea that cyberspace should remain free from any regulation cannot be seriously sustained. In recent years, public authorities have partially succeeded in conscious attempts to enforce the rule of law on the Internet. While international efforts to reach common standards and cooperation remain modest, some progress has been made especially in the area of child pornography and copyright infringement. But for the most part, public authorities have focused on the enforcement of their own legal rules. In this respect, European policy has been mainly oriented towards Internet services providers, seeking their cooperation in the search for and the removal of illegal material. Under the threat of being fined or held liable for damages by national court rulings, ISPs as business operators, are eager to take advantage of the conditional exemption of liability regime in the new e-commerce Directive by taking down unlawful data when being enjoined or even informally notified to do so. After the *Yahoo!* case major American ISPs that were at first reluctant to commit themselves to censorship now seem ready to remove or disable access to controversial material that is prohibited by European standards but hosted in the US – despite the protection offered by the First Amendment of the American Constitution. Human rights activists are now in possession of more efficient weapons to fight the spread of hate and racist speech on the Internet. However, the "notice and take down" system equally affects other kinds of controversial or unorthodox speech that fully deserve to be

displayed' and 'Regrettably, in some cases this policy may prevent users from accessing items that do not violate the law. At this time, we are working on less restrictive alternatives. Please accept our apologies for any inconvenience this may cause you, and we hope you may find other items of interest on Ebay" (Rosenbaum, *o. c.*).

57 "German official asks U.S. ISPs to block neo-Nazi sites", *CNN.com*, August 29, 2000.

58 "Regierungspräsident wehrt sich gegen Zensurvorwürfe", December 8, 2001, *Heise online.*

protected. The current alliance between state policy and business interests creates a serious risk of massive and arbitrary censorship, which is not consistent with the protection allowed to speech by the European Convention for the protection of human rights and fundamental freedoms. It is not enough to get the ISPs to do the job of the police, it is also necessary to give them guidelines defining the limits of the right to free speech and offering procedural guarantees against censorship. Business operators, even stimulated by economic incentive, should never be entrusted with these principles, which belong to the very core of the human rights of a democratic people.

Oxford, January 2002