

## **Strategies to Tackle Racism and Xenophobia on the Internet – Where are we in Europe?**

### ***Keynote address in***

### **Racist and Xenophobic Content on the Internet – Problems and Solutions**

***Organised by the Institut für Informations-, Telekommunikations- und Medienrecht (ITM) in cooperation with Landesanstalt für Medien Nordrhein-Westfalen (LfM)***

**Düsseldorf, October 31, 2002**

### **1. Introduction**

Racism, xenophobia and incitement online are part of Internet content regulation. The problem to regulate content on the Internet is at least twofold : the criminalization of the content and the effective enforcement of the criminal law.

Today, some kinds of content, such as child pornography or copyright infringements, are clearly criminalized according to international standards. Other types of content, such as those said to be “harmful to youth”, are more tricky : they do not in themselves breach the law and cannot, therefore, be blocked or taken down altogether.

With respect to racism and xenophobia, one of the specific challenges arises from the fundamental clash between the U.S. and Europe. The same speech might indeed be allowed on one side of the Atlantic while, at the same time, being firmly prohibited on the other side.

The First Amendment of the U.S. Constitution states that “*Congress shall make no law (...) abridging the freedom of speech, or of the press (...)*”. According to the case law of the U.S. Supreme Court, racist and xenophobic propaganda are constitutionally protected as varieties of controversial political speech. Public authorities are therefore forbidden from interfering in the content of such communications.

In Europe, the situation is entirely different. According to article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms and the case law of the European Court of Human Rights, the right to free speech does not extend to speeches that threaten,

*Dr. Isabelle Rorive*

*Centre for Comparative Law (Université Libre de Bruxelles)*

*Programme in Comparative Media Law & Policy's collaborator (Oxford University)*

*irorive@ulb.ac.be*

deny or even lead to the destruction of human dignity and human integrity. No protection is either given to speeches that directly incite harm or advocate violent behaviour against other human beings. The European Convention states in full words that none of its provisions can be understood to imply for anyone the right to engage in an activity that aims at destroying other people's rights and freedoms (article 17).

Such standards are consonant with the international Covenant on Civil and Political Rights adopted by the U.N. in 1966. On the lines of the European Convention of Human Rights, the international Covenant defines the right to free speech as a qualified right, i.e. a right which entails duties and responsibilities (article 19).

The strong European view is spreading in the common law world if one considers two recent cases dealing with revisionist propaganda. In Canada, the Human Rights Tribunal decided on January 18, 2002, in the famous *Zundel case*<sup>1</sup>, that the Holocaust denial site hosted in the U.S. but maintained in Canada by Ernest Zundel was unlawful. In the same line stands a decision held in Australia on September 17, 2002<sup>2</sup>. The Federal Court of Australia enjoined Mr. Toben, the director of an important revisionist research and publishing centre, the Adelaide Institute, to remove offensive material posted on the Web.

With respect to Europe, there is an important point to stress out. If national legislations prohibit and generally penalise racist and xenophobic speech, there are still important disparities between these legislations. For instance, the denial of crimes against humanity is an offence in only four E.U. countries, namely Germany, Austria, France and Belgium.

The E.U. has recently decided to address this question. In November 2001, the Commission issued a proposal for a Council framework decision on combating racism and xenophobia<sup>3</sup>. This proposal -which is expected to be adopted by the end of 2002- aims at harmonising anti-racist legislations. It sets severe criteria. On the one hand, its scope is fairly broad : racism and xenophobia is defined as "*the belief in race, colour, descent, religion or belief*,

---

<sup>1</sup> *Ernst Zundel v. The Queen* [2002] 2 S.C.R. 731 at <<http://nizkor.org/ftp.cgi/people/z/zundel.ernst/supreme.court/judgement.1992>> (last visited on November 21, 2002).

<sup>2</sup> *Jones v. Toben* [2002] FCA 1150 (September 17, 2002) at <[http://www.austlii.edu.au/au/cases/cth/federal\\_ct/2002/1150.html](http://www.austlii.edu.au/au/cases/cth/federal_ct/2002/1150.html)> (last visited on November 21, 2002).

<sup>3</sup> November 28, 2001, COM (2001) 664 final, 2001/0270 (CNS) at <[http://europa.eu.int/comm/employment\\_social/news/2002/feb/proposal\\_jai\\_664\\_en.pdf](http://europa.eu.int/comm/employment_social/news/2002/feb/proposal_jai_664_en.pdf)> (last visited on November 21, 2002).

*national or ethnic origin as a factor determining aversion to individuals or groups*” (article 3 (a)). On the other hand, the offences it covers are also extensive. They include : 1° public incitement to violence or hatred for racist or xenophobic purposes ; 2° public insults or threats racially motivated ; 3° denial or trivialisation of crimes against humanity ; 4° public dissemination or distribution of material containing expression of racism and xenophobia, by any means, including the Internet (article 4).

Considering the clash of values between Europe and the U.S. -or should I say, between the main part of the world and the U.S.-, at least four questions come to mind when one thinks about racist speech online :

- Should racist content be regulated at all on the Internet?
- Should national anti-racist laws be applied to the Internet? And, in any case, is it feasible or realistic to apply national laws online?
- Should the Internet be governed through international regulation?
- What is the appropriate role of the intermediaries in the picture?

## **2. Regulation of racist content on the Internet**

It is not long ago that, *de facto*, the Internet was escaping from any anti-racist regulation. The hate sites, for the most part hosted in the U.S., were considered as unreachable and the general policy was to put up with the situation. This is in line with the position defended by free speech advocates according to whom the Internet should remain a sphere of complete and absolute freedom, unrestrained from any regulation whatsoever. Here, the debate is about the suitability of the regulation itself.

At the same time, European authorities, as well as national governments and NGOs fighting racism and discrimination have been confronted with the dramatic growth of the hate business online. In this respect, the Simon Wiesenthal Centre described as “problematic” more than 2,300 Web sites hosted in the year 2000 in the U.S. were they are legally protected. Among them more than 500 were allegedly authored by Europeans. Today, the number of such “problematic” web sites exceeds 3000. According to recent figures released by the Council of

Europe, amongst the 4,000 xenophobic websites listed around the world, more than 2,500 are hosted in the U.S. Furthermore, the Council of Europe pointed out that only 160 of these websites did exist in 1995<sup>4</sup>.

Such a growth of the hate business online coupled with the fact that Europe has now more Internet users than the U.S. and Canada together -Europe has almost 186 million users, while Canada and the U.S. register 182 million, and Europe is still a growing market<sup>5</sup>- called for the coming back of the law online.

### 3. Application of national anti-racist laws to the Internet

National States have accordingly tried to apply their own legislations to the Internet, upon the principle “what is illegal off-line is illegal online”. Then again, there is a huge gap between the national scope of States’ sovereignty and the universality of cyberspace where national borders have been until now of little relevance. In this respect, the *Yahoo! case* is a major instance. In 2000, a French judge ordered Yahoo! Inc. to take all appropriate measures in order to prevent people located on the French territory from accessing its auction sales of Nazi paraphernalia and, more broadly, from accessing any pro-Nazi site hosted on its servers (mainly, on *Geocities*)<sup>6</sup>. In November 2001, at the request of Yahoo! Inc., a U.S. federal District Court declared that the First Amendment precludes enforcement within the U.S. of the French ruling<sup>7</sup>. An appeal of this decision is currently pending before the U.S. Court of Appeals for the Ninth Circuit<sup>8</sup>. At the same time, former Yahoo! CEO, Tim Koogle, has been

---

<sup>4</sup> Council of Europe (Committee on Legal Affairs and Human Rights), report in the general assembly on the Draft additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Doc. 9538), rapporteur : Ignasi Guardans, September 5, 2002, point 8 at <http://assembly.coe.int/Main.asp?link=http://assembly.coe.int/Documents/WorkingDocs/doc02/EDOC9538.htm> (last visited on November 21, 2002).

<sup>5</sup> According to Irish-based industry monitor Nua.com (figures released in September 2002).

<sup>6</sup> TGI Paris (emergency proceedings), November 20, 2000 at [http://www.droit-technologie.org/4\\_1.asp?jurisprudence\\_id=21](http://www.droit-technologie.org/4_1.asp?jurisprudence_id=21) (last visited on November 21, 2002).

<sup>7</sup> *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 at

<http://www.juriscom.net/en/txt/jurisus/ic/dccalifornia20011107.htm> (last visited on November 21, 2002).

<sup>8</sup> See the court documents at <http://www.cdt.org/speech> (last visited on November 21, 2002).

sued before a French criminal Court for apologetics of war crimes and crimes against Humanity. Jurisdiction has already been asserted but a verdict has not been reached so far<sup>9</sup>.

When considering the *Yahoo!* case, it is quite patent that the coexistence of conflicting forums leads to a legal chaos and a jurisdiction dead-end. This is a real challenge today. In order to tame this legal chaos, projects to “renationalize” or to “zone” the Internet are cropping up. The idea is to avoid legal problems and extra-costs caused by the various national laws and to set up new technical devices that would allow to “format” Internet content to each legal system. But, with such technical devices, the Internet as a global forum is going to vanish. In addition, choosing such a path is somehow backing non-democratic States which are eager to prevent their own people from accessing any controversial information and opinion coming from the outside.

#### **4. International standards dealing with racism and xenophobia**

A logical way to escape this jurisdiction dead-end would be to agree on international standards regarding racist and xenophobic speech. As a matter of fact, international law provides such standards. A provision of the 1966 international Covenant on Civil and Political Rights states that “*any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law*” (article 20-2). This obligation has been specified in the U.N. Convention on the Elimination of all Forms of Racial Discrimination, in force since 1969. This Convention provides that States Parties “*shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination (...)*” (article 4 (a)). In 2001, the U.N. Conference against racism held in Durban made perfectly clear that this prohibition should apply to the Internet.

However, these international provisions do not bind the United States of America, which have consistently made constitutional reservations regarding the obligation to outlaw racist speech. The Council of Europe tried to deal with this problem in the Convention on Cyber-crime, adopted in November 2001 and signed by 30 European countries along with Canada,

---

<sup>9</sup> TGI Paris, 17e chamber (press chamber), February 26, 2002, RG n° 0104305259 at < [http://www.droit-technologie.org/4\\_1.asp?jurisprudence\\_id=102](http://www.droit-technologie.org/4_1.asp?jurisprudence_id=102)> (last visited on November 21, 2002).

Japan, South Africa and, last but not least, the U.S.. The Cyber-crime Convention includes some content-related offences, namely child pornography and copyright infringements. Former drafts also included hate speech, but the U.S. delegation made clear that such provision would contravene the First Amendment and prevent them from signing the Treaty. As a compromise, it was decided to make these controversial provisions subject to a separate Protocol which will be open for signature at the end of January 2003<sup>10</sup>. As a matter of fact, the U.S. will certainly refrain from signing this Protocol. At present, there is no international agreement with the U.S. on racist speech standards, either off-line or on-line, and such an agreement seems extremely unlikely to be reached.

## 5. Role of the intermediaries in the regulation of racist content on the Internet

A last solution is to ask the Internet Services Providers (ISPs) to self-regulate racist and xenophobic material posted on-line or to co-regulate such content in collaboration with public authorities. In the U.S., the Congress passed on the so-called “Good Samaritan provision” - included in the 1996 Communication Decency Act (section 230-c-2)<sup>11</sup> - which protects ISPs that voluntarily take action “*to restrict access to or availability of material that (they ...) consider to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable (...)*”. This provision undoubtedly covers racist and xenophobic speeches. In practical terms, this means that U.S. ISPs are allowed to suppress or to block this kind of material despite the fact that it is constitutionally protected. Furthermore, the same statute also immunised ISPs in respect of illegal, damaging or harmful material, stored or disseminated by them but authored by others. U.S. courts have applied this provision in an extensive manner. They ruled that the hosting provider will not be held liable even if it was aware or the unlawful character of the content, even if it had been notified of this fact by the victim and had done nothing about it, and even if it had paid for the controversial material. In other

---

<sup>10</sup> Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of racist and xenophobic nature committed through computer systems, adopted by the Committee of Ministers on November 7, 2002 at <[http://www.coe.int/T/E/Legal\\_affairs/Legal\\_co-operation/Combating\\_economic\\_crime/Cybercrime/Racism\\_on\\_internet/PC-RX\(2002\)24E.pdf](http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/Racism_on_internet/PC-RX(2002)24E.pdf)> (last visited on November 21, 2002). This Additional Protocol will be open for signature on the occasion of the next Parliamentary Assembly session of the European Council (27-31 January 2003).

<sup>11</sup> CDA 47 U.S.C. at <<http://www4.law.cornell.edu/uscode/47/230.html>> (last visited on November 21, 2002).

words, ISPs in the U.S. are exonerated from any liability in tort whether they decide to take down controversial material or to leave it available on the Internet.

In Europe, the matter was handled in a different way by the e-commerce Directive, which is in force in the E.U. Member States since January 17, 2002<sup>12</sup>. The regime set up by the Directive applies to the circulation and the storing of racist and xenophobic data as well as to incitement to hatred and to violence. This Directive also creates “safe havens” for the sake of ISPs, but it leaves some room for public interventions and allows the States to impose duties on ISPs.

As a matter of principle, the Directive states that ISPs cannot be obliged to monitor the Internet nor to seek for illegal activities on the web (article 15).

However, a Member State may compel them to inform public authorities about illegal data and infringements reported by the recipients of their services. ISPs may also be obliged to communicate information enabling the identification of their subscribers at the authorities’ request. Moreover, the Directive explicitly mentions the possibility for national courts and administrative authorities to enjoin both access and hosting providers to filter or to remove illegal material, such as racist and xenophobic speeches (articles 12.3 and 14.3). This possibility has been used by president Jürgen Büssow - the President of the Government of the County (Regierungsbezirk) of Düsseldorf- who enjoined access providers established under his jurisdiction to block access to Nazi and racist sites hosted abroad, mostly in the U.S.. Such an order was made under the threat of a fine up to 200,000 Euros. Similar measures have occasionally been taken elsewhere. In Switzerland, for instance, where the police put a former important U.S. based pro-Nazi gateway (*Front14.org*) on a “black list” voluntarily abided by ISPs. Many other countries are familiar with such a practice. However, black lists are more commonly used with respect to criminal sexual material (such as child pornography). On the contrary, the French judge of emergency proceedings who condemned Yahoo! Inc., did not, in the so-called *J’accuse case* decided in 2001<sup>13</sup>, consider that there was

---

<sup>12</sup> 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) at <[http://europa.eu.int/ISPO/ecommerce/legal/documents/2000\\_31ec/2000\\_31ec\\_en.pdf](http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf)> (last visited on November 21, 2002).

<sup>13</sup> TGI Paris (emergency proceedings), October 30, 2001, R.G. n° 01/57676 at <[http://www.droit-technologie.org/4\\_4.asp?pays\\_id=2](http://www.droit-technologie.org/4_4.asp?pays_id=2)> (last visited on November 21, 2002).

a legal ground on the basis of which he could enjoin the French access providers to filter the Nazi portal *Front.14*. hosted in the U.S..

The E.U. Directive also provides a new tool that does not work as a stick (like fines or court orders) but as a carrot. Article 14 of the Directive states that the hosting provider will not be liable in relation to the unlawful material that it has been storing as long as it is not aware of its illegal character. However, as soon as it obtains such a knowledge, it must take immediate action to block or to remove this material in order to keep the benefit of the immunity. This provision incites hosting providers to voluntarily take down illegal material whenever they are notified, either formally by public authorities or informally by a watchdog, a victim or any private party, about the illegal data. The new tool provided by the e-commerce Directive is very efficient for combating hate speech in particular, since ISPs are eager to ensure the benefit of immunity. This is also true with respect to the U.S. ISPs which are international business operators and, as such, often have assets in Europe besides a reputation to care for. In this line, the German Federal Office for the Protection of the Constitution (*Bundesamt für den Verfassungsschutz*) notified e-Bay, the world largest e-shopping website, which is based in California, about the sale of Nazi-related songs, books, clothing and paraphernalia on its auction site. Contrary to Yahoo!, e-Bay each time reacted positively to the notice and promptly disabled access to the controversial items. Moreover, eBay formally declared in May 2001 that it “*will no longer host the sale of memorabilia from the Nazi period or anything related to fanatical groups*”.

The combination of the E.U. Directive provisions, on the one hand, and the U.S. “Good Samaritan” provision, on the other hand, allows the Europeans to play behind the back of the Constitution of the United States of America. It strongly incites U.S. based ISPs operating internationally to apply an anti-hate speech policy consistent with the standards of international law<sup>14</sup>.

Up to now, we have seen that the e-commerce Directive induces two strategies for the Member States to get rid of racist material online : either, they ask the European-based access

---

<sup>14</sup> For further details, see B. Frydman and I. Rorive, “Free speech and liability of intermediaries on the Internet in Europe and the United States of America”, *Zeitschrift für Rechtssoziologie* [Journal for Sociology of Law of the Cologne Max Planck Institute], 2002, vol. 23 (1), p. 41-59, sp. 55-56.



providers to filter the illegal content, or they manage to convince the U.S.-based hosting provider to remove the illegal content from the Net altogether.

But there is a third possible strategy, which consists neither to block access nor to urge for a take down but to target and to pressure the search engines (like Google, Altavista, *etc.*). Though search engines are unable to prevent direct access to a site of interest, an exclusion from a search engine may nonetheless have a similar effect on a site's ability to reach its intended visitors. Enjoining a search engine to stop linking to "problematic" websites is unquestionably an efficient method since most of Internet users find websites and link to them through a search engine. At the same time, this strategy seems quite straightforward to implement, as there are only a handful of powerful search engines in use amongst Internet surfers around the world, and especially in Europe. Therefore, search engines are increasingly becoming the key-players in the regulation of illegal content online.

A report from the Berkman Center for Internet and Society of Harvard University, released on October 24, 2002<sup>15</sup>, shows that the famous California based company Google has **quietly** excluded 65 sites from listings available at Google.de. and 113 from listings available at Google.fr. Most of these sites are anti-Semitic, pro-Nazi or related to white supremacy (e.g. *stormfront.org*). Has also been banned "*Jesus-is-lord.com*", a fundamentalist Christian site that is adamantly opposed to abortion. In a press interview, Google spokesman, Nate Tyler, said : *"To avoid legal liability, we removed sites from Google.de search results pages that may conflict with German law"*<sup>16</sup>. He indicated that each site that was de-listed came after a specific complaint from a foreign government, but he refused to hand down a list of the targeted websites.

As a matter of fact, search engines have to be particularly cautious since they are not covered by the e-commerce Directive. This means that they fall outside the regime of exemption of liability set up by the Directive with respect to access and hosting providers. Today, the regime of liability of search engines remains uncertain. Article 21-2 of the e-commerce Directive provides that the Commission shall, before June 17, 2003, examine *'the*

---

<sup>15</sup> J. ZITTRAIN and B. EDELMAN, *Documentation of Internet Filtering Worldwide* (Berkman Center for Internet & Society, Harvard Law School) at <<http://cyber.law.harvard.edu/filtering>> (last visited on November 21, 2002).

<sup>16</sup> D. MCCULLAGH, "Google excluding controversial sites", *CNET News.com*, October 23, 2002 at <<http://news.com.com/2100-1023-963132.html>> (last visited on November 21, 2002).

*need for proposals concerning the liability of providers of hyperlinks and location tool services*". In any case, it seems that Google has decided to play safely and to follow official complaints from European authorities.

## **6. Conclusion**

Cyber-racism raises questions about, on the one hand, retaining the Internet's enormous capacity to share information freely and to provide a public space to discuss controversial issues and, on the other hand, about the responsible use of that public space in a manner which does not undermine basic human rights.

Through co-regulation, we have now in Europe more or less efficient tools to combat racism and incitement on-line. In this respect, one has to emphasise the role played by hotlines and watchdogs, which help to find and to track problematic websites and whose role is essential in the implementation of the policy of public authorities.