Racism, Xenophobia and Incitement Online:
European Law and Policy

Hate.com

The Internet allows the communication of all kinds of information and ideas at a level and at a speed that have never been reached in the past. At the same time, it facilitates the massive spread at low cost of problematic messages such as racist and xenophobic propaganda and incitement to hatred and violence. The Simon Wiesenthal Centre described as “problematic” more than 2,300 web sites hosted in the year 2000 in the U.S. where they are legally protected. Among them more than 500 were allegedly authored by Europeans. Today, the number of such “problematic” Web sites exceeds 3000.

European authorities, as well as national governments and NGOs fighting racism and discrimination, are deeply concerned about the dramatic growth of the hate business online and the free access to Web sites and newsgroups that are illegal in most European countries.

- Simon Wiesenthal Centre, “Problematic Sites on the Internet”<http://www.wiesenthal.com/problematic_sites/>
U.S. Constitutional Protection

The First Amendment of the U.S. Constitution prevents the Congress, and by extension any public authority, from interfering in the content of communications that take place in a public forum.

Racist and xenophobic propaganda are thus constitutionally protected in the U.S. as varieties of controversial political speech. As a consequence, a public authority cannot forbid the selling of Nazi paraphernalia online or a Web site promoting white supremacist theories, for instance. Freedom of speech does not however cover “fighting words”, which by their very utterance inflict injury or tend to incite an immediate breach of the peace.

The U.S. Supreme Court has granted the Internet, unlike Radio and Television, the full protection of the First Amendment (Reno I, 1997). This does not affect the right of private actors, like universities, business corporations and Internet services providers (ISPs), to impose their own standards and terms of service on their students, employees and consumers.

- U.S. Constitution: First Amendment
  <http://caselaw.lp.findlaw.com/data/constitution/amendment01/>
  <http://supct.law.cornell.edu/supct/html/00-795.ZS.html>
  <http://www.hofstra.edu/Academics/Law/law_lawrev_kubler.cfm>

European Ban on Racist Speech

In Europe, article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms and article 11 of the E.U. Charter of Fundamental Rights also protect freedom of speech as a basic right and as an essential foundation of a democratic society.
Nevertheless, freedom of speech is not absolute. It may be subject to certain limitations and even penalties, so as to justify the intervention of public authorities in order to protect *inter alia* the public safety or the rights of other people.

As a result, racism and xenophobia, as well as incitement to hatred or violence, do not fall within the right to free speech in Europe. On the contrary, they are prohibited and penalised in most national legislations.

Material posted on the Internet does not escape from such regulations. The latter may be applied to online data, not only when the illegal content is hosted in the country or authored by a national citizen, but also when it is considered to be “published” in the country. This generally means as soon as it is accessible via a computer located on the state territory.

In the last few years, European citizens have been prosecuted and punished, in a significant number of criminal cases, arisen in several European jurisdictions, for posting on the Internet messages of a racist and xenophobic nature or messages inciting to hate or violence.

  [<http://www.echr.coe.int/Convention/webConvenENG.pdf>]

- Charter of Fundamental Rights (E.U., 2000): Art. 11  
  [<http://ue.eu.int/df/docs/en/CharteEN.pdf>]

- Instances of European cases dealing with racism and xenophobia:
  - Belgium: First instance Tribunal of Brussels, December 22, 1999  
    [<http://www.droit-technologie.org/4_1.asp?jurisprudence_id=33>];  
    Appeal Court of Brussels, June 27, 2000  
    [<http://www.droit-technologie.org/fr/4_1.asp?jurisprudence_id=11>];  
    First instance Tribunal of Brussels, January 15, 2002  
    [<http://www.juriscom.net/txt/jurisfr/cti/tpibruxelles20020115.htm>]
  - France: cases dealing with racist and revisionist content on the Internet between 1996 and 2002 at  
    [<http://www.juriscom.net/txt/jurisfr/cti/resum.htm#UEFJ>]
  - Germany: S. Gold, “German Landmark Nazi Ruling”, *Newsbytes*,  
    December 12, 2000  
    [<http://www.computeruser.com/news/00/12/14/news5.html>];  
    P. Bartlett, “Germany Struggles with Neo-Nazi Websites”, *BBC news*,  
    December 22, 2000  
    [<http://news.bbc.co.uk/hi/english/world/europe/newsid_1083000/1083049.stm>];  
    “Nazi Leader’s Grandson Fined Over Online Quotes”,  
    *Yahoo!News*, January 24, 2002  
E.U. Framework Proposal on Racism and Xenophobia

In November 2001, the Commission issued a proposal for a Council framework decision on combating racism and xenophobia. This proposal aims at criminalizing racist conduct and speeches in the same way through all the European Union. It will ensure that the various national anti-racist legislations are sufficiently comprehensive and severe and that effective judicial cooperation can be developed within the E.U. It also sets minimal criteria with regard to jurisdiction.

The scope of the text is fairly broad: “racism and xenophobia shall mean the belief in race, colour, descent, religion or belief, national or ethnic origin as a factor determining aversion to individuals or groups” (art. 3 (a)).

The offences covered by the proposal are also extensive. They include public incitement to violence or hatred for racist or xenophobic purposes, public insults or threats racially motivated and denial or trivialisation of crimes against humanity. The proposal also criminalizes the “public dissemination or distribution of tracts, pictures or other material containing expression of racism and xenophobia” (art. 4 (e)), by any means, including the Internet. It is based upon the principle “what is illegal off-line is illegal on-line”.

- Proposal for a Council Framework Decision on combating racism and xenophobia (EU, Brussels, 28 November 2001)  

International Standards

Many other democracies around the world (like Australia, Canada, India, etc.) share the European legal position on racism, xenophobia and incitement to violence. The latter is also consistent with the provisions of International Law.

The International Covenant on Civil and Political Rights protects freedom of speech as a right “which carries with it special duties and responsibilities” (art. 19). Furthermore, this fundamental text makes a specific exception with respect to hate speech. According to article 20-2, “any advocacy of national, racial or
religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law”. Such an obligation to proscribe has been specified and extended by the International Convention on the Elimination of all Forms of Racial Discrimination, in force since 1969 and undertaken by most European countries (art. 4 (a)).

These international provisions do not however bound the U.S. which have consistently made constitutional reservations regarding the obligation to outlaw racist speech.

In 2001, the U.N. Conference against racism held in Durban came to the conclusion that “at the outset of the third millennium, a global fight against racism, racial discrimination, xenophobia and related intolerance and all their abhorrent and evolving forms and manifestations is a matter of priority for the international community” (Declaration: point 3). Moreover, it was recalled that “the dissemination of all ideas based upon racial superiority or hatred shall be declared an offence punishable by law” (Declaration: point 86). With regard to the Internet, deep concern was expressed about the use of new information technologies “for purposes contrary to respect for human values, equality, non-discrimination, respect for others and tolerance, including to propagate racism, racial hatred, xenophobia, racial discrimination and related intolerance” (Declaration: point 92).

- The Declaration of the World Conference against racism, racial discrimination, xenophobia and related intolerance (U.N., Durban, August 31 - September 8)<http://unhchr.ch/html/racism/Durban.doc>

The Cybercrime Convention

The International Convention on Cybercrime was adopted by the Council of Europe in November 2001 and has already been signed by 30 European countries, along with Canada, Japan, South Africa and the U.S. With respect to content-related offences, the Convention fosters international prosecution of child pornography and copyright infringements, but does not extend to hate speech and incitement to violence. This is due to pressure from the U.S.
delegation, which made clear that such a regulation would contravene the First Amendment of their Constitution and prevent them from signing the treaty. As a compromise, it was decided to make these controversial provisions subject to an additional Protocol of which the final draft was released in May 2002.

The First Additional Protocol to the Convention on Cybercrime obliges the parties to criminalize “distributing or otherwise making available racist and xenophobic material to the public through a computer system” (art. 3-1). Racist and xenophobic material is defined as “any written material, any image or any other representation of thoughts or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors” (art. 2-1). The Protocol also covers racist and xenophobic threats or insult (art. 4 and 5) as well as the denial, gross minimisation, approval or justification of genocide or crimes against humanity (art. 6).

The Council of Europe is also preparing a Second Protocol to the Convention on Cybercrime covering “terrorist messages and the decoding hereof”. According to a press declaration made by the head of the economic crime division of the Council of Europe (Peter Csonka) in February 2002, this text will address “how to identify, how to filter, and how to trace communications between terrorists”.

- Second Additional Protocol to the Convention on Cybercrime:
  - E. Launet, Interview of the Council of Europe Secretary General: “The aim is to harmonise criminal law”, Libération, March 9, 2002 <http://www.coe.int/T/E/Communication_and_Research/Press/Theme_Files/Cybercrime/e_InterviewSGLiberation.asp>
The Yahoo! Case

In 2000, at the request of two NGOs fighting racism and anti-Semitism, 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).

Yahoo! immediately challenged the French decision in the U.S. In November 2001, a federal district Court declared that the First Amendment precludes enforcement within the U.S. of the French ruling. An appeal of this decision is currently pending before the Court of Appeals for the Ninth Circuit.

Striking back, another French NGO sued former Yahoo! CEO, Tim Koogle, 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.

In the meantime, Yahoo! banned hate-related goods (Nazi and KKK items in particular) from its auction site and removed numerous, but not all, pro-Nazi Web pages from Geocities.

- Briefs, reports and rulings in the French civil Yahoo! case <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522-asg.htm>
- Briefs and rulings in the U.S. civil Yahoo! case <www.cdt.org/jurisdiction>
- Webibliography on the civil Yahoo! case <http://www.lapres.net/html/yahweb.html>
- Some press comments and other literature on the civil Yahoo! case:
The Büssow Policy in Germany

The conflicting standards on hate speech and the jurisdiction dead-end emphasised by the Yahoo! case actually make European regulations on racism and xenophobia go unheeded on the Internet. The problematic data hosted in the U.S. appears at first sight out of any European control. Though authors and hosts are difficult to reach, another way is to target European ISPs and to compel them to filter the hate data they give access to.

In Germany, Düsseldorf district government president Jürgen Büssow has gone down such a path. All ISPs established on his territory have been ordered to block access to a list of Nazi and racist sites based in the U.S. under the threat of a fine up to 200,000 €. Since then, users trying to access the banned sites have been redirected to the government Web site where they are told about German law and the local government policy.

Similar measures have occasionally been taken elsewhere, in Switzerland, for instance, where the police put a very 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 generally restricted to criminal sexual material (such as paedophilia).

- Papers in German on *Heise online*:  
  <http://www.heise.de/newsticker/data/hod-08.10.01-001/>;  
  <http://www.heise.de/newsticker/data/em-28.05.01-000/>

**U.S. ISPs’ Liability Regime**

As a matter of fact, ISPs are key actors in the implementation of the regulation proscribing racism, xenophobia and incitement to violence on the Internet. National authorities often ask ISPs to play an active role in the struggle against illegal content online. In addition, ISPs have been sued and sometimes been found liable in court, as publishers or accomplices, for illegal data they hosted or gave access to.

The U.S. Congress reacted as early as 1996 and immunised all providers of interactive computer services from any civil liability in tort with respect to material stored or disseminated by them but created by others (*Communication Decency Act, 230 (c) (1)*).

At the same time, the Congress passed on the “Good Samaritan provision” (*C.D.A., 230 (c) (2) (A)*), backing the ISPs that voluntarily decide to exert editorial control or apply content-based restrictions of speech. This clause stated 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.” Racist and xenophobic speeches are certainly included in this extensive list.

- Sections 230 (c) (1) and 230 (c) (2) (A) of the 1996 Communication Decency Act (1996, *C.D.A. 47 U.S.C.*)  
  <http://www4.law.cornell.edu/uscode/47/230.html>
• With respect to copyright infringements, see the distinctive regime set up in the Digital Millennium Copyright Act (1998, D.M.C.A. 17 U.S.C. 512 (C)) : new section 512 added to the 1976 Copyright Act
<http://www.loc.gov/copyright/legislation/hr2281.pdf>

**E.U. ISPs’ Liability Regime**

The E.U. e-commerce Directive, in force since January 2002, also created “safe havens” for the sake of ISPs, i.e. conditional exemptions from civil and criminal liability. This particular liability regime is of general application. It clearly relates to the circulation and storing of illegal racist and xenophobic speeches or incitement to hatred and violence.

Regarding “mere conduit”, ISPs cannot be held liable for data they transport or give access to when they play only a passive role (art. 12).

Hosting providers are also safe as long as they ignore the illegal content they are keeping on their server. After obtaining such knowledge, they could be held liable if they do not act expeditiously so as to remove or to block access to the unlawful data (art. 14). The knowledge may be the result of an informal notice by either a public authority, like the police, or a private party, like a watchdog or any recipient.

As a matter of principle, ISPs cannot be imposed a general obligation to monitor Internet content or to actively seek for illegal activities. But the States may compel them to promptly inform public authorities about illegal data or infringements reported by recipients of their services. The States may also oblige ISPs to identify their subscribers at the request of public authorities (art. 15).

Moreover, the Directive explicitly mentions the possibility for national courts and administrative authorities to enjoin both access and hosting providers to prevent or to put an end to a breach of the national law (art. 12.3 and 14.3). As a result, ISPs could still be obliged to block questionable data when asked to do so, such as in the Yahoo! ruling or in the Büssow injunction.

External Effects of the E.U. Policy

From the combination of conditional “safe havens” shaped in the e-commerce Directive with the “Good Samaritan” provision embodied in the U.S. law, U.S. based ISPs are given a strong incentive to implement European free speech standards whenever they carry out business in Europe, run a subsidiary there or owe in one way or another some assets on the old Continent. In ruling out or taking down racist and xenophobic speeches, they simultaneously enjoy the benefit of immunity in Europe and in the U.S.

The efficiency of this new tool has, for instance, been striking in a case involving eBay, the largest shopping Web site based in California. The German Federal Office for the Protection of the Constitution (Bundesamt für den Verfassungsschutz) notified eBay twice, in 2001 and 2002, about the sale of Nazi-related songs, books, clothing and paraphernalia on its “marketplace”. Contrary to Yahoo!, the company each time reacted positively to the notice and promptly disabled access to the controversial items. In addition, eBay formally declared that it “will no longer host the sale of memorabilia from the Nazi period or anything related to fanatical groups.”

- Literature on the eBay story:
  - A. Rosenbaum, “Nazi Items Gone from Ebay Under German Pressure”, Newsbytes, January 17, 2002 <http://www.infowar.com/class_1/02/class1_011802a_j.shtml>

From Regulation to Self-Regulation

The European regime of liability limitations is less comprehensive than the U.S. C.D.A. immunity clause and it imposes more duties on ISPs. More room is also left to States’ intervention, a position consistent with the specific European approach to freedom of speech as a qualified right.

At the same time, the e-commerce Directive opens wide the door towards self-regulatory and co-regulatory initiatives. Unlike
the U.S. Digital Millennium Copyrights Act (D.M.C.A., 1998) dealing with copyright infringements and the recent Japanese statute on ISPs liability limitations (Law N° 137, November 30, 2001), the E.U. Directive does not set up a formal “notice and take down” procedure, so as to widen the scope for best practices and negotiated agreements.

The Directive stresses that the Member States and the Commission shall encourage the drawing up of codes of conduct “regarding the protection of minors and human dignity” (art. 16-1 (e)), which includes the issue of racism and incitement to discrimination. In this respect, Members States and the Commission shall support the involvement of associations and organizations in the drafting and implementation of those codes (art. 16-2).

By Prof. Benoit Frydman and Dr. Isabelle Rorive
Programme in Comparative Media Law and Policy
Oxford University – Wolfson College
bfrydman@ulb.ac.be - irorive@ulb.ac.be

*