ECRI

European Commission against Racism and Intolerance
Commission européenne contre le racisme et l'intolérance

CRI (2000) 27

European Commission against Racism and Intolerance

LEGAL INSTRUMENTS TO COMBAT RACISM ON THE INTERNET

Report prepared by the Swiss Institute of Comparative Law
(Lausanne)

Strasbourg, August 2000

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Secretariat of ECRI
Directorate General of Human Rights – DG II
Council of Europe
F - 67075 STRASBOURG Cedex
Tel.: +33 (0) 3 88 41 29 64
Fax: +33 (0) 3 88 41 39 87
E-mail: combat.racism@coe.int

Visit our web site : www.ecri.coe.int

LEGAL INSTRUMENTS TO COMBAT RACISM ON THE INTERNET

PROBLEM OF THE DISSEMINATION OF RACIST MESSAGES VIA THE INTERNET:

GENERAL CONCLUSIONS OF ECRI

The following general conclusions, which are based on the report on legal measures to combat racism on the Internet prepared for the European Commission against Racism and Intolerance (ECRI) by the Swiss Institute of Comparative Law, were adopted by ECRI at its 22nd plenary meeting (13-16 June 2000) and transmitted by ECRI to the European Conference against Racism (Strasbourg, 11-13 October 2000).

1. The Internet is a powerful tool for combating racism and intolerance on a worldwide scale. It offers an unprecedented means of facilitating the cross-border communication of information on human rights issues related to anti-discrimination. The use of the Internet to set up educational and awareness-raising networks in the field of combating racism and intolerance is a good practice which should be supported and further developed.

2. However, alongside these positive uses, the Internet also represents a source of concern, in that it is being used by individuals and groups to disseminate racist messages, inciting to intolerance and racial and ethnic hatred.

3. ECRI commissioned the Swiss Institute of Comparative Law (Lausanne) to carry out research into existing legal measures to combat racism on the Internet. This research demonstrated that the Internet, like any other means of communication, does not fall outside the scope of the law. The real cause for concern is not so much that there is an absence of relevant legal provisions, as the fact that the very nature of the Internet may block their full implementation. In particular, the diffused structure of the Internet, its pervasiveness and the possibility it affords for anonymity, may render difficult the enforcement of legal provisions.

4. Having studied the findings of the aforementioned study, ECRI underlines the necessity of making a distinction between the function of access provider and that of host provider and of clearly establishing their respective responsibilities. While the access provider should be held liable for illegal content of which it was aware and which it had not blocked, the host provider should have a wide duty of diligence as regards especially those sites which it hosts anonymously and free of charge.

5. ECRI, for its part, stresses the importance of including the issue of combating racism, xenophobia, antisemitism and intolerance in all current and future work at international level aimed at the suppression of illegal content on the Internet. ECRI recalls that the fundamental principle of respect for human dignity calls for the fight against dissemination of racial hatred and against incitation to racial hatred.

6. ECRI is aware that the way in which the balance between the freedom of expression and the right to protection against racial discrimination is managed differs widely between countries. It is also aware that many racist sites originate in the United States. ECRI is of the opinion that a dialogue should be initiated with all providers, particularly US providers, in order to discuss measures to counter racist sites. Such measures, which could be entered into on a voluntary basis by providers, might include blocking sites, a filtering system or refusing anonymity to the authors of sites.

7. ECRI is furthermore convinced that the control of parties working in the Internet field, such as access and host providers, should be based to a large extent on self-regulatory measures. In this respect, ECRI encourages the development of codes of conduct to which all such parties could subscribe.

8. ECRI considers that the prosecuting authorities in most European countries are not adequately trained to deal with the problem of the dissemination of racist messages via the Internet and that concerted efforts should therefore be made in this direction. A further problem is that of inefficient international legal co-operation on this issue. Ways should therefore be found to strengthen such international co-operation and mutual assistance between the law enforcement services across the world.

9. In this respect, ECRI is of the opinion that the setting-up of a co-ordinatory body, which would act as a permanent monitoring centre, mediating body and partner in the preparation of codes of conduct, would be a positive step forward.

10. ECRI stresses the need for more active awareness-raising among the general public concerning the problem of the dissemination of racist messages via the Internet. Special attention should be paid to raising awareness among young Internet-users – particularly children – that they may come upon racist sites and the potential risks of such sites.

11. ECRI fully supports the anti-racist initiatives which already exist on the Internet and strongly encourages co-operation between existing anti-racist web sites, as well as the development on the net of new sites devoted to the fight against racism and intolerance.

12. ECRI is of the opinion that strengthened co-operation between the member States of the Council of Europe on the issue of the dissemination of racist messages via the Internet and the harmonisation of their national practices on this subject would be a welcome addition to the range of activities already underway to combat racism, xenophobia, antisemitism and intolerance. Member States might wish to send a strong message at the European Conference against Racism in October 2000, in the context of the European preparations for the World Conference which is to take place in October 2001: the message being that the European region is determined to take action to ensure that the Internet is not used to racist ends and to develop rather its potential as a tool for intercultural communication, understanding between the peoples of the world and the spread of a universal human rights culture.

SUMMARY

INTRODUCTION

Terms of reference

On 19 August 1999 the Council of Europe formally commissioned the Swiss Institute of Comparative Law, Lausanne, to produce a report on the legal measures, in particular criminal-law measures, intended to combat racism on the Internet. The study was to be based on the situation in a dozen member countries of the Council of Europe: Germany, Austria, Belgium, Estonia, France, Italy, Norway, Poland, the Czech Republic, Russia, Sweden and Switzerland.

The terms of reference were defined at a meeting between the Deputy Director of the Institute and the European Commission against Racism and Intolerance (ECRI) held in Strasbourg on 15 June 1999. A member of the Institute who attended a meeting of the Internet Sub-Committee of the ECRI held in Paris on 5 November presented a progress report and the object of the research was further refined.

On 31 March 2000, within the agreed period, the Institute submitted the present Report to the ECRI in a bilingual version, partly in French and partly in English.

Scope of the study

Our first observations in this regard concern the fact that the terms of reference were confined to *criminal law*: this limitation was justified by the fact that this branch of the law is the best suited to combat hateful words. Having said that, we considered it appropriate to make the occasional reference to civil law or administrative law, which sometimes offer effective means, particularly from the aspect of speed, of ensuring that access to racist sites is blocked, or indeed that these sites are simply closed down.

It will be noted that the study concentrates on *legal* measures to combat racism on the Internet. The word "legal" must be understood in a broad sense, however, and is not restricted solely to positive law, consisting of legal rules and judicial decisions. In a sphere as mobile and unstable as Internet law (see the caveat below) the majority of countries covered by the study have combined the classic normative approach with the measures deriving from soft law. Although there was no express provision to that effect in the terms of reference, the Institute considered that it could not disregard these more flexible instruments consisting of codes of conduct, ethical requirements, recommendations or hot lines, if not because of their effectiveness, at least because of their strategic importance.

As regards the classic approach, it should be emphasised at the outset that the rules specifically aimed at racism on the Internet – or even more generally at abuse of freedom of expression on the network of networks – are virtually non-existent. Admittedly, there is no shortage of proposals, whether from legal commentators or from the authorities; but in order to avoid overdiversification and confusion (owing to

the frequently divergent and contradictory nature of these proposals), we have made a point of dealing only with proposals which are in the process of being adopted; in other words, those being debated in Parliament.

It should further be noted that judicial decisions on the matter are also still rare; and they do not constitute a body of settled case-law, since with few exceptions the only judgments delivered thus far have been those of the lower courts. In order to compensate for this lacuna, the study takes into account judicial decisions delivered in other cases involving unlawful expression on the Internet, in particular pornography and infringement of copyright. The fact that the relevant issues, beginning with the delicate question of the "subsidiary" liability of technical operators (access providers and hosts) means that such an extension of the scope of the investigation is valid, and indeed necessary.

Does this extension of the material scope of the study make up for the reduction of its geographical scope? The reader will note that this report says virtually nothing about the situation in the four central and eastern European countries referred to in the mandate (Estonia, Poland, the Czech Republic and Russia). This relative silence is not due to forgetfulness on our part or to the absence of racist messages on the networks of those countries; in fact, we redoubled our efforts to contact the bodies concerned with racism on the Internet in these countries (prosecution authorities, access providers and human rights organisations) – to no avail. No specific provision in that regard was reported, whether of the classic normative type or soft law[1]. There is an explanation: the development of the network of networks is still at a very embryonic stage in these countries, where the Internet is still the prerogative of an academic elite.

Finally, the study will also deal with the situation at European Union level. Not that the EU is in the process of mounting a direct attack on the problem of racism on the Internet: that is by no means the case. None the less, the directive on electronic commerce, which is in the process of being adopted, establishes certain standards concerning the liability of technical intermediaries: these standards will be binding on Member States and will have some effect on the fight against the distribution of illegal contents, including racist contents.

Working procedures

We decided not to present a compilation of reports on a country-by-country basis, since the reader would eventually have been lost in the jungle of national specificities, primarily institutional and procedural. We therefore opted for a horizontal approach, which provides a better means of comparing problems and attempted solutions.

We therefore begin by setting out the various technical and legal difficulties associated with seeking the persons committing offences involving racist expression. We then examine the possibilities of imposing liability on actors other than the person actually committing the offence, first by means of classic legal measures and then by soft law measures. After briefly considering the provisions of international law measures which may be relevant, the study ends by summarising the problem and,

1 However, the principal access providers, which are subsidiaries of foreign companies such as IBM, AT&T in Croatia or FREEnet in Russia, refer to the codes of conduct of their parent companies, which in the majority of cases are American.

in particular, briefly lists the instruments which we consider appropriate or inappropriate. In all cases our general considerations are illustrated by examples of significant developments in one or other of the countries studied.

Before we get to the core of the subject, however, we feel it necessary to describe certain technical data; in particular, it is important to define the role played the various actors involved in the process of disseminating communications on the Internet; similarly, it is worth mentioning the various services offered by the Internet. These differences give rise to nuances and distinctions in the legal regime applicable.

Finally, we must point out that the present study does not review the various criminal provisions of the countries concerned aimed at combating racism in general. That information is available in an earlier report by the Institution, also commissioned by the Council of Europe, entitled *Legal measures to combat racism and intolerance in the member States of the Council of Europe*, which was published by the ECRI in 1998 and is also available on the Internet[2].

Caveat

The myth of an Internet without faith or law should be dismissed at the outset. This myth of a legal vacuum, which is supported by certain alarmist politicians, amplified by the press and exacerbated by unconsidered declarations of independence by "surfers" eager for absolute freedom, does not stand up to examination. Like any other means of communication, the Internet does not escape the law. As a general rule, the laws governing the right of communication are drafted in a technically neutral manner, which takes into account any dissemination of information irrespective of the medium; consequently, they are fully applicable to messages distributed on the Internet. As we shall see, the problem therefore lies not so much in the absence of adequate material rules as in obstacles to their application in the form of the characteristics peculiar to the network of networks, namely its polycentric structure, its ubiquity and the cover of anonymity.

This is all the more so because, returning to racist expression, our previous report showed that all European countries have at their disposal a more or less effective legislative arsenal to repress hateful expressions. This minimum standard, moreover, is imposed by the United Nations Convention on the Elimination of All Forms of Racial Hatred, Article 4 of which requires the adoption, inter alia, of a provision penalising the propagation of racial hatred outside a strictly private circle. These criminal provisions, which are drafted in general terms, are applicable, inter alia, to hateful expressions disseminated via the Internet.

2 http://www.ecri.coe.int/fr/03/03/f03030001.htm

There is an exception to the common standard, however; it concerns negationism, which means calling in question the existence of genocide. Other than France, where it is an offence to "dispute crimes against humanity",[3] only Switzerland, Germany, Belgium and Austria punish this offence; and in the latter three countries the offence is limited to the denial of genocide committed by the Nazis. This difference in approach is worth mentioning, out, since revisionist sites are flourishing on the Internet.

Finally, the reader's attention should be drawn to a last point of importance: the changing, or rather ephemeral, nature of the present study. Technology develops very rapidly – who, at the beginning of the 1990s, could have predicted the lightning development of the Internet? – and the law on communications, despite struggling to keep pace, is also developing very quickly. Perhaps the problems described here will no longer be problems in a few years, indeed in a few months; in addition, the solutions recommended are equally volatile. From this aspect, it should finally be noted that the various websites referred to in the footnotes are up to date on 20 March 2000.

3 Article 24 bis of the Law of 29 July 1881, as amended by the Law of 13 July 1990.

I. INTERNET: THE TECHNICAL AND LEGAL ENVIRONMENT

It is appropriate to point out a number of factors of a factual, in particular technical, nature, without which it is not easy to understand why the fight against unlawful, and more particularly racist, contents on the Internet gives rise to new difficulties for lawyers, difficulties which have not always been overcome by the legislature and especially by the courts, which are often incapable of precisely distinguishing the various facets of Internet communication and their implications. In some cases the Internet is referred to as software, in others access providers have been confused with hosts, while in yet others courts have declined to adjudicate on the matter. Nowadays such hesitations or errors of assessment are becoming less common, owing in particular to better training for the competent authorities. It none the less remains that the terminology is not yet uniform and there is still a risk of confusion, in particular from one language to another.

1.1. The characteristics of the network of networks: polycentrism, ubiquity, secrecy, transience

Polycentrism: First of all, the Internet is not a centralised network but a distributed network, i.e. is a collection of different and varied networks (academic, commercial, regional etc.) joined together by links; devices connected to one or other of these multiple networks can communicate among themselves by using common technical languages (protocols). This absence of centralisation has an important consequence: it is impossible to intervene by taking action against any "head" of the network, which would pass an injunction down through the various subordinate levels until it reached the final level. In real terms, an injunction to a specific access provider to cut off access to a racist site would prevent access to that site only by surfers connected to the Internet through the access provider on which instruction was served. Where action is aimed at the entire network of networks, it is necessary to contact directly the undertaking whose server *accommodates* the impugned statements (and there may be several of these in the case of mirror sites, i.e. sites accommodated elsewhere which replicate the content of the original site).[4]

Ubiquity: As a network of networks, the Internet has a global dimension. The communications which it carries are in principle accessible from any point on the planet which is connected to the network of networks. In practice, a racist message distributed on the Internet is therefore potentially visible from everywhere, regardless of the location of the server which accommodates and distributes it. None the less, some services are reserved for authorised persons (who use a password) or accessible only on payment of a fee. Similarly, certain closed networks, known as Intranets, are of a strictly local

4 Note: contrary to what the general public willingly believe, the Internet Society (http://www.isoc.org/isoc) is not a managing body of the network of networks (it cannot be repeated enough: there is no such body) but an international group of surfers whose aim is to promote the development of the Internet in the sense of the sharing of knowledge and free communication at world level.

nature; they use the techniques which have made the Internet successful (in particular hyperlinks) but serve only the specific addressees of a precise entity (an undertaking or a university, for example); the wide public of surfers cannot access them, in the absence of an interconnection; having said that, a racist message is reprehensible whether it is disseminated on the Internet or an Intranet, because it is disseminated outside a strictly private circle (except in the rather theoretical case of an Intranet limited to a restricted circle of close acquaintances).

Secrecy: for various reasons surveillance of the network of networks is very difficult. First, it is possible to communicate anonymously on the Internet: many sites allow surfers to obtain software allowing them to send or consult messages in complete confidentiality; either they eliminate all trace of connections or they conceal the identity of the computer used.[5] Significantly, all machines linked to the network are identifiable, since when a machine is connected it is allocated an individual Internet address (known as the IP address and consisting of a series of numbers). The situation is therefore similar to that applicable to road traffic: each vehicle has an individual registration plate, although the driver as such is not identifiable.

The secret nature of the Internet is reinforced by the fact that certain unlawful contents are disseminated in an encrypted form. In other words, the content of a message is comprehensible only to those who have the decoding key (which is not always the same as the encoding key). However, the restrictions on the right to encode applicable in a few rare countries (notably France), like the more widespread restrictions on the export of encryption software (notably in the Unites States) undoubtedly hinder the possibilities of circulating messages with illicit contents.

Finally, the surveillance of communications is also made more difficult by the fact that, as the technique of dissemination means, the data which go to make up a single message are not necessarily circulated together; the information is split up into several packages, which often take different routes. This makes interception, in particular the legal interception, of unlawful communications more difficult.

Transience: information – whether a short message or voluminous files – travels very quickly on the Internet. In a few seconds racist messages forced to disappear from one server may reappear on another server on the other side of the world. Such a relocation makes virtually no difference to the surfer: in view of the ubiquity of the Internet, he accesses it as before, immediately the new access address is known.

5 See, for example, http://www.anonymizer.com/3.0/index/shtml. These sites are not specifically intended to promote crime on the Internet but to prevent personal information from being collected and personality profiles of surfers from being drawn up for essentially commercial purposes.

1.2. The services offered

It is important to realise that the Internet is simply a technique which allows separate networks to interoperate. On these networks various forms of services circulate, and they may come under the legal regime applicable to individual communication, that applicable to the press or that applicable to radio and television broadcasting. However, the following services are the most common and the most specific:

Electronic messaging: better known under the English name "e-mail", this service is comparable to the traditional mail sent by post. It is reserved to "point-to-point" communications, that is from a specific sender to a (or sometimes a number of) specific addressee(s). Owing to its private nature, any racist messages sent via this medium are in principle lawful, since in the countries studied racial propaganda or hateful statements constitute an offence only where they are disseminated *in public*; however, e-mail may sometimes convey circular letters to a large number of addressees, in which case they will no longer be in the nature of private communications exempt from legal proceedings.

Electronic mailboxes: these services permit the exchange of all sorts of contributions (selective remarks, articles, images etc.) on a given topic. These "multilog" services, known as new groups, mailboxes, discussion groups or discussion lists, may be supervised by a "moderator" or uncontrolled, and offered only to approved participants or completely public. In principle, contributions are erased after a certain period (calculated in days, weeks or months, depending on circumstances); some services offer archives which allow "dead" contributions to be consulted. "Chat rooms" are similar to discussion groups, apart from the fact that the conversation takes place in real time; users are required to register and use nicknames to identify themselves.

www sites: these sites are storage places for information whose size varies between a few paragraphs and dozens of pages containing text, graphics, images or even sound. They are interlinked by hypertexts which make it possible to switch automatically from one site to another and are the basic components of the vast web that is the Internet. It is thus significant that racist sites all have lists of links to other sites of the same type, which make it easy to navigate in the universe of hateful expression.

It should be noted that:

- these services are increasingly combined. One www site may offer a discussion group which makes it possible to extend the discussion of the topics dealt with by the site and a messaging service which allows direct contact between users and those in charge of the content of the site.[6] This convergence is accentuated by the fact that some sites also offer multi-media products which makes them very similar to a traditional broadcasting service.

6 See, for example, the well-known racist site www.stormfront.org, which offers all kinds of racist texts, moderated and unmoderated discussion groups, a chat service, the opportunity to contact the publishers (comments@stormfront.org) and, finally, hypertext links to a host of www sites of the same type.

- in legal terms, setting up a www site, a discussion group, a discussion list or a chat room, and participating in these various services, are not subject to any particular formality or control; such administrative measures, moreover, would scarcely be compatible with freedom of expression. Under French law, however, anyone setting up a www site is required to make a declaration (declaration of an audio-visual service).

1.3. The actors

First of all, a distinction must be drawn between the providers of the containers and the providers of the contents. The former make available the infrastructure which makes communication on the network of networks possible; they have no influence over the content of the various messages which they convey. The latter have direct influence over the content of the messages, whether because they are the authors or publishers of the messages or because they participated in their formal conception. Between these two poles there is yet a third, more flexible, category, which brings together actors who, in various ways, act as relays for the contents.

Be that as it may, it should be emphasised that this typology is schematic in nature. First, it is not uniformly accepted; in certain countries the actors are known by different titles, with the attendant risks of terminological confusion. Then, and in particular, an ever-increasing number of operators combine the various roles, and provide the infrastructures, access, host services and information services at the same time.

1.3.1. The providers of containers

The telecommunications operator: its role is restricted to setting up the necessary terrestrial or radio telecommunications network and conveying information on this network, which may be a traditional telephone network, a wide-band integrated network or a cable broadcast distribution network. In the countries studied this economic activity is subject to administrative authorisation for reasons to do with the scarcity of broadcasting channels and the more or less marked public-service nature of the services provided. The telecommunications operator merely conveys millions of messages per day and in principle assumes no responsibility for any unlawful dissemination. For this reason no further reference to this actor is necessary.

The access provider: this person plays a key role in communications on the Internet. It provides surfers with the indispensable connection to the network of networks, on the basis of a contract, which is most often lined with general conditions. This economic activity is not subject to administrative authorisation; it follows that it is not possible to carry out a general surveillance of the way in which the access provider functions; in particular of the nature of the sites to which it provides access.

The host: the host provides a content provider with a storage and data-management service (hard disk space, machine processing and tape loop capacity) which allows the information to be accessible, notably via a dedicated www site. It may also undertake to provide technical assistance or information on the number of connections or files downloaded. Relations between the host and subscriber are contractual; here, too, general conditions generally complete supplement contractual terms. It may also be the case that the host participates directly in designing the site by providing its "pages" (graphic design, creation of frames etc.).

1.3.2. The providers of contents

Apart from the **author of the statements or images**, who is beyond doubt the principal actor, this category consists of:

the value-added provider: generally, he offers services or information on the Internet (databases, games, news bulletins, advertising etc.)[7].

the surfer: this is the person who navigates; at first sight he is essentially a consumer of the contents, but in certain cases (discussion groups in particular) he also provides information.

1.3.3. The relayers of information

This category combines various actors who, although they have no direct influence on the content of the messages, none the less play an important role in locating, updating it and selecting information, such as those who run on-line archives and "monitor" discussion groups or establish hypertext links to other information sources. In principle, because they operate the "points", these persons are aware of the information to which they point. However, it may happen that the information which they highlight is altered without their knowledge (the hypertext link remains the same, but the content of the site has changed).

7 Anglo-saxon terminology tends to group the host and the value-added supplier under the generic term *service provider*.

II. LEGAL ISSUES INVOLVED IN THE WORK OF LAW ENFORCEMENT AND INVESTIGATION AUTHORITIES

The Internet, being characterised by the volatility and ubiquity of its contents (refer to Part I above), constitutes an important challenge to law enforcement authorities. Although the Internet is not a legal vacuum and the responsibilities of its actors are defined or definable (refer to Part III, below), the traditional instruments used by law enforcement authorities to establish such responsibility, i.e. tracing the actors and producing evidence of criminal acts, are not necessarily adapted to the specific technical features of the Internet. In what follows, we will analyse the scope of competence of national law enforcement authorities, the procedures they must respect in pursuing investigations and the limits of their investigative powers deriving from basic rights of the individual (data protection) and other constitutional guarantees. Apart from problems existing at the internal level, the lack of international co-operation in the area and the fact that certain countries have turned into safe harbours for hate-oriented speech, due to far going protection of the freedom of expression, constitute serious obstacles to the work of law enforcement authorities.

2.1. Jurisdiction: the wide scope of territorial competence

The Internet constitutes a global means of communication that allows users to access information from all over the world. A question arises as to the extent to which individual national authorities are competent for contents originating from outside the national territory.

2.1.1. Jurisdiction in Criminal Matters

In criminal matters, most countries subscribe to the principle of territorial jurisdiction, according to which the competence of national law enforcement authorities is limited to crimes committed on national territory. The place at which a criminal offence was committed is, in most countries, defined in two ways: either the place where the illegal act was committed, or the place where the result of the illegal act was felt. Given the latter part of the definition, most countries are theoretically competent for any illegal content on the Internet, provided that is accessible from their territory[8].

Germany

According to § 9 of the German Penal Code (*Strafgesetzbuch*, hereinafter *StGB*), the location of a criminal act is defined as the place where the criminal

8 See also Report of the Council of Statet, "*Internet et les réseaux numériques*", 1998, p. 167, http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm.

acted or where the result of his action materialised or was intended to materialise.

France

Under the Criminal Code, French law is applicable to offences committed on the territory of the Republic. An offence is deemed to have been committed on the territory when at least one of its constituent elements has taken place in the sea, land or air space of the French Republic (Art. 113-2).

Italy

Article 6 of the Criminal Code lays down the principle of the territorial application of criminal law: any person who has committed an offence on Italian territory is liable to be punished according to Italian law. Article 6 paragraph 2 states that an offence is to be regarded as having been committed in Italy where the act or omission took place there, in whole or in part, or where the event resulting from that act or omission was produced there (ubiquity).

These examples show that national provisions concerning territorial jurisdiction give States a very broad jurisdictional competence. The French Conseil d'Etat described the situation as follows:

> "It follows from those provisions that French criminal law clearly applies in the case of an offending message available on the Internet network, no matter where in the world its source is situated ... Such a mechanism in reality has the effect of dissociating the place where the offence was actually committed from the place where it produces its effects, and gives the national courts a very broad jurisdiction.[9]"

This very broad competence is considered problematic in some states, because it forces anyone who publishes on the Internet to check all the legal orders of the world if he or she wants to be sure that his publication will not constitute a criminal offence. For this reason, and because such legal uncertainty may constitute obstacles to economic development in the area of Internet services, attempts have been made in some spheres to restrict the general rules on criminal jurisdiction when these are applied to Internet.

Germany

Legal commentators propose to limit criminal jurisdiction in respect of the Internet to those acts with which the author really intends to reach a German audience[10]. Only contents tailored to a German audience should fall within German jurisdiction.

European Union

The proposed Directive on electronic commerce[11] effectively limits jurisdiction to the country of origin of the service provider (Art. 3 of the Directive). The

---

9 Report of the Council of State, cited in footnote 8 above, p. 167.

10 See Collardin, Straftaten im Internet, Computer und Recht 1995, p. 618 (621).

11 To be found on: http://www.ispo.cec.be/Ecommerce/legal/legal.html.

service provider can only be held responsible according to the legal provisions in force at the place of his business[12]. However, by way of derogation, the Member States may take measures for the purpose of fighting incitement to hatred on grounds of race, sex, religion or nationality (Art. 22, para. 2 of the Directive).

2.1.2. Jurisdiction in civil matters

Jurisdiction in civil matters concerning the Internet is much less clear than criminal jurisdiction. In the fight against racism on Internet, civil jurisdiction becomes relevant where the author of illegal content can be held responsible on the basis of tort law, which means that he is either liable in damages (for example in Italy; refer to Part III, below), or the addressee of a cease and desist order. Where the access or host provider cannot be held responsible under criminal law, a civil law cease and desist order aimed at cutting access to an Internet site with racist content can be an efficient alternative means of stopping the distribution of such racist content.

As in criminal cases, a question arises as to the extent of the competence of the national court when the author and/or Internet host of the racist content is located in a foreign country[13].

Italy

In the only Italian decision[14] to deal with the question of the international jurisdiction of an Italian court in respect of an unlawful act committed on the Internet, the President of the court granted an application for an injunction concerning defamatory information published on an "open" Internet site, although the server was in the United States. The respondent's argument that the Italian court lacked jurisdiction was rejected on the ground that the court was competent to deal with a complex activity involving the dissemination of information which was harmful to others, since this information, by being placed on the website, was directly accessible in all countries linked to the Internet. Accordingly, the fact that the website concerned was opened abroad and the information loaded abroad could not preclude the jurisdiction of the Italian courts.

Once the competent court is determined, there arises a more complicated question as to which law a judge must apply when deciding about the legality of content on a server located abroad. The diversity of rules existing in this regard entails the risk that a domestic judgment will not necessarily be enforced in the foreign country where the illicit content is stored on a server. Harmonisation of rules would minimise this risk.

---

12 More details: Spindler, Multimedia und Recht 1999, 199, 206.

13 According to the Brussels Convention of 1968 and the Lugano Convention of 1988, of which most of the European States are members, the victim can choose between a court in the country of the defendant's domicile or a court in the country where the damage was caused or a court in the country where the damage arose. Of course the conventions only apply when the defendant is domiciled in one of the States Parties to the conventions.

14 Order of the President of the Teramo District Court of 11 December 1997 (civil matter, action for an injunction, case of defamation), in Diritto dell'informazione e dell'informatica 1998, p. 370.

2.2. The existence of safe data harbours, especially freedom of speech in the US

Although, in theory, states are competent for the prosecution of Internet crimes committed anywhere on the globe, they will not succeed in holding responsible the person who published illegal content if this material was posted to the net in a country where such content is protected by law. In respect of racist content, due to a very broad conception of the freedom of speech, the United States of America has become a safe data harbour in which prosecutions in respect of racist content or the enforcement of any foreign judicial decision will be extremely difficult. The fact that a majority of racist sites are located in the US makes it necessary to explain the US-American concept of freedom of speech in more detail.

Although the United States has actively pursued a policy agenda intended to combat behavior motivated by hatred[15], the fight against hate motivated communications on the Internet faces some specific obstacles. These communications are classified as speech in the American legal system and, as such, the special protection accorded to freedom of speech by the First Amendment to the United States federal Constitution[16] makes the regulation of their content extremely difficult. As a result, and despite numerous attempts, there is currently no comprehensive federal legislation prohibiting racism on the Internet.

The importance of free speech has historical roots. The founders of the United States came to America to avoid persecution - often at the hands of their own governments - for their political or religious ideas. Their goals in establishing a new system of governance were to guarantee individual freedom and to place strict controls on those in power. Censorship - particularly of ideas which might be unpopular – was anathema to a truly democratic process and was therefore to be eradicated at all costs.

Even now, freedom of speech is seen as the most fundamental of rights in the United States. The theory most frequently advanced is that only through open public debate will the truth become clear. Such debate is possible only if no ideas, no matter how unpleasant, are censored. This public debate - in particular the ability to be informed about and to criticize the government as well as majority-held opinions - is an essential prerequisite for all citizens to perform their self-governing function. The specter of legal sanctions imposed on a particular type of speech might have a "chilling effect" on legitimate speech: an individual might refrain from stating his opinions for fear of punishment, thereby depriving the public of this point of view.

In order to protect the individual's rights from governmental censure, the American legal system requires judges to verify the constitutionality of any law under which an accused may be prosecuted. In order for the government to be able to regulate an area, not only must adequate legislation be drafted and enacted, such legislation must pass the judicial test of constitutionality before it can be enforced.

---

15 Heather De Santis, *Combatting Hate on the Internet: An International Comparative Review of Policy Approaches,* Strategic Research and Analysis SRA-350, Department of Canadian Heritage, 1998, p.31.

16 "*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." (*italics added*) USCA Const. Amend. I.

In particular, a law which places any restriction on the freedom of speech is subject to the strict scrutiny of the courts. The restriction must be clearly defined, justified by a compelling interest of the government and limited to what is strictly necessary[17] to achieve the specific goal. Restrictions based on the content or subject matter of speech might allow the Government to effectively silence certain ideas and are therefore presumptively unconstitutional.

2.2.1. Federal legislation

Only in the area of obscenity have courts tended to find that government interests in regulation outweigh the primacy of free speech[18]. That fact, combined with strong political pressures concerning the protection of children from cyberporn, may explain why the only pieces of legislation attempting to regulate the content of Internet communications adopted on a federal level to date have targeted indecent rather than racist communications.

The first such attempt was the Communications Decency Act of 1996[19] (CDA) which provided for both civil and criminal penalties for the use of an interactive computer service to knowingly transmit, send or display certain material of a sexual or excretory nature to minors. The U.S. Supreme Court held significant provisions of the CDA to be unconstitutional[20] as they related to "indecent" or "patently offensive" materials on the grounds that it was not the least restrictive means to achieve the government's goals. Other provisions, in particular those providing certain defenses to liability for service providers and those prohibiting communication of obscene e-mails intended to harass or annoy its recipient[21], remain in force.

Congress subsequently adopted the Child Online Protection Act (COPA) which targets commercial websites that disseminate information "harmful to minors" without restricting underage access to such materials[22]. COPA represents Congress' attempt to remedy the constitutional defects in the CDA. COPA's constitutionality has, however, been challenged as being vague and overbroad because it threatens speech that is protected as to adults. A federal district court has granted a preliminary injunction against enforcement of COPA on the ground that COPA is presumptively invalid as a content-based regulation of non-obscene sexual expression[23].

---

17 Supreme court opinions have generally referred to this element as requiring that legislation be "narrowly tailored" (as opposed to being "overbroad") and that it represent the "least restrictive means" for achieving the government's goal.

18 John F. McGuire, *When Speech is Heard Around the World: Internet Content Regulation in the United States and Germany,* 74 NYULR 750, 753 (1999).

19 Publ. L. N° 104-104, 110 Stat 133 (codified in scattered sections of 47 U.S.C.)

20 Reno v. ACLU, 117 S. Ct. 2329 (1997) (invalidating portions of the Communications Decency Act of 1996 as not representing the most restrictive means to achieve the government's goals).

21 ApolloMedia Corp. v. Reno, 1998 WL 853216 (U.S. (Cal.) 1999) amended by 119 S. Ct. 1459 (US 1999) as cited in *Andrews Computer & Online Industry Litigation Reporter* "High Court Upholds Law Banning 'harassing' or 'annoying' e-mail" May 18, 1999.

22 COPA provides for fines and/or imprisonment for whoever knowingly makes a communication for commercial purposes by means of the World Wide Web that is available to any minor that includes any material harmful to minors. Publ L. 105-277 112 Stat. 2681-736 codified as 47 U.S.C. §231.

23 ACLU v. Reno, 31 F.Supp2d 473 (E.D. Penna. 1999)

2.2.2. State legislation

State laws specifically prohibiting racist expression have not generally survived claims of unconstitutionality. For example, in *R.A.V.* v. *St. Paul*[24], the U.S. Supreme Court struck down a city's ordinance that made it illegal to exhibit a burning cross, a swastika, or other inflammatory symbol that might arouse "anger, alarm, or resentment in others on the basis of race, color, creed, religion or gender". All nine justices agreed that such acts were reprehensible, but that the ordinance was unconstitutional. There was, however, considerable disagreement concerning the rationale supporting the judgment, and the case generated four separate published opinions.

Other laws, particularly those concerning fair housing and employment, which do not specifically target racist speech have sometimes been used successfully to prosecute or prohibit racist speech. The California Supreme Court, for example, has held that racist comments directed at an employee by his superior may even, in some circumstances, be subject to a prior restraint. Where such comments "contribute to a hostile or abusive work environment" and therefore constitute employment discrimination, such speech may be enjoined at the workplace[25].

Although few state laws specifically address communications over the Internet, courts are generally willing to apply existing doctrines, such as employment and housing discrimination, to electronic messages. Two lawsuits for employment discrimination have recently been filed based on the circulation at the workplace of racist e-mails[26]. Although neither suit has yet reached a trial on the merits, one has survived a motion to dismiss[27]. The Pennsylvania Attorney General sought an injunction against a white supremacist group and all persons and entities having control of that group's website in connection with threatening material against an individual on that site[28], and federal authorities subsequently filed charges for civil rights violations[29]. Defamation statutes have been used when a specific individual is targeted, or in states which have enacted group libel statutes.

Other legal theories that have been used include harassment, ethnic intimidation, and mental distress of a person to whom abusive language is address or hearing abusive language addressed to another. The issue in these cases "invariably turns on the issue of whether the language in question is so outrageous that society wishes to permit recovery, and this requires an examination of the nature of the language at issue in particular cases . . . Recovery has tended to be permitted in such cases where the plaintiff has been placed in reasonable fear of physical harm or of some other clearly intimidating experience such as arrest or imprisonment."[30]

---

24 505 U.S. 377 (1992).

25 Aguilar v. Avis Rent A Car System, Inc. 87 Ca. Rptr.2d 132 (Ca. S.Ct. 1999).

26 Owens v. Morgan Stanley & Co., 1997 WL 403454 (S.D.N.Y. 1997); Curtis v. Citibank, 1998 WL 3354 (S.D.N.Y. 1998).

27 Owens v. Morgan Stanley & Co., 1997 WL 793004 (S.D.N.Y. 1997).

28 "AG'S Complaint Says Hate Group Published Terroristic Threats on the Internet", *The Legal Intelligencer Vo.219, N° 79*, October 21, 1998

29 "Feds Target Web Threats", *The National Law Journal Vol 22, N° 23,* January 31, 2000.

30 "Civil liability for Insulting or Abusive Language – Modern Status", *American Law Reports ALR 4th, Vol. 20 (1983) Current through the September, 1999 Supplement.*

First Amendment law is a highly controversial area of American law, particularly as it concerns expressions of racism, and it poses a classic case of the competing imperatives of liberty and equality. The *raison d'être* of the First Amendment guarantee of freedom of speech is the protection from persecution of those holding a minority view. Yet it's strict application creates serious obstacles to the protection of certain minorities from verbal abuse. The development of the Internet - in particular the ability to reach an increasingly large audience while remaining totally anonymous and therefore free from editorial or societal pressures - has added a new level of complexity and urgency to the fight against racism in the United States.

This problem of "safe havens" is not limited to racist contents, but also concerns revisionist sites whose existence has to do with the fact that there is no criminal legislation in that regard in certain European countries.

2.3. The legal basis for investigations and seizures

The criminal or civil responsibility of a particular author of illegal content can only be established on the basis of evidence. The volatility of electronic content confronts the investigative authorities with major difficulties (refer to point 2.2., above). They are expected to react fast, whereas the legal means of intervention do not effectively permit quick intervention or seizure of evidence in most countries. The prerequisites for obtaining a search warrant are very often ill adapted to the form which illegal content takes on the Internet. Moreover, the technical means for an efficient investigation, based on tracing data transfers back to the author, are very often in the hands of the access or host provider. This poses the question of whether access providers are obliged to help police in the process of obtaining or securing relevant data files. Another limitation on tracing back illegal content, especially in the field of e-mail, is the fact that surveillance of the private communication is only possible within the narrow scope of the laws on the interception of postal and telephonic communications.

Austria

To be able to search a building, police officers require - as in most countries – a judicial search warrant (139 ff StPO). Having gained access to a building, police may seize material which is relevant to the investigation, including data files and computers. The owner of any data base is obliged to co-operate for this purpose. Co-operation can consist of production of copies of data files, decryption of encrypted messages or processing data in such a way that it can be used by the law enforcement authorities. Moreover, according to § 89 of the Telecommunications Act, the operators of telecommunication services are obliged to provide to the police all the installations which are necessary for the surveillance of telecommunications. On the other hand, access providers, other than public institutions, who know of the existence of illegal content, are not obliged to bring it to the attention of the authorities (§§ 84 and 86 of the Criminal Procedure Act).

European Union

Art. 5 of the Telecommunications Data Protection Directive requires that interception or monitoring of communications, on both public and non-public networks, take place only when legally authorised.

Germany

As in other countries, police may seize materials which are linked to the commission of a criminal offence. However, they may not seize e-mails which are held in intermediate storage on the server of an access provider. The storing of e-mails is still part of the communication process, so that seizure would have to be qualified as an interception of telecommunications. Under a constitutional guarantee (Art. 10 Grundgesetz) such an interception of telecommunications can only be effected by the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*) or by the corresponding institutions of the *Länder*. In a case decided by the Regional Court of Hanau[31], a public prosecutor was forbidden to seize incoming and outgoing e-mails which were still stored on the server of the access provider. The prosecutor had ordered their confiscation because he suspected orders for pornographic materials to be among them.

Concerning certain extremely serious criminal offences, Internet providers are obliged to inform the authorities of the planning or commission of such an offence (§ 138 StGB). The offence of incitement to racist hatred, however, does not rank among them.

United Kingdom

The main legislation which permits British police to search for evidence of an offence committed by use of the Internet is the Police and Criminal Evidence Act 1984 (Chapter 60 of 1984). Under Part II of that Act, police are normally required to obtain a warrant from a Justice of the Peace if they wish to enter premises in order to search for and seize evidence of an offence having been previously committed. A first prerequisite is that there be "(...) reasonable grounds for believing" that a "(...) serious arrestable offence" had been committed (subpara. 8(1)(a)). To use words or display written material that is intended or likely to stir up racial hatred is an arrestable offence under subsec. 18(3) of the Public Order Act 1986. Whether the offence is "serious" must be evaluated by the judge on each application. Secondly, the police must show either that they would be unable to obtain access to the premises or the evidence without the warrant (subparas. 8(3)(a)-(c)), or that asking for access would probably result in the destruction or disappearance of the evidence (subpara. 8(3)(d)). One imagines that this will often be the case with respect to racist material, particularly if it is stored on computers for distribution over the Internet. Para. 5 of Schedule 1 to the Act provides that, in cases where the material sought is "contained in a computer", then the search warrant shall be interpreted as an order obliging the person in possession of the material to produce it in a visible and legible form in which it can be taken away by the police. Thirdly, the police must describe, as closely as is practicably possible, the individual articles which they believe exist and which they wish to seize (subpara. 15(2)(c)). The warrant permits entry to the specified premises on only one occasion (subsec. 15(5)). In the result, if the police are to obtain authorisation to seize evidence of propogation of racist material, they must first find out by other means that a relevant offence has been committed.

31 LG Hanau, Beschluss vom 23.9.1999, NJW 1999, S. 3647.

Hence the importance of information provided by Internet users via hotlines or other means of information. Once a warrant has been obtained, the police can seize anything on the premises searched which amounts to evidence of any offence that has been committed. Subsec. 19(4) specifically authorises the police to "require any information which is contained in a computer and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible". Nevertheless, the police find these statutory constraints frustrating in the context of racism on Internet, as they do not permit the police to maintain ongoing surveillance of what material is being propagated by known racists or racist groups from time to time[32].

The Public Order Act 1986 makes additional provision for the police to be able to search for and seize material which is specifically in breach of sec. 23 of that Act, namely material that is likely to stir up racial hatred and is in the possession of the accused for the purpose of being distributed, shown or played. Under subsec. 24(1), such a search operation can only be conducted upon the authority of a warrant issued by a Justice of the Peace and it is up to the police to show reasonable grounds for suspecting that a person has a racist writing or recording in his possession. There is no guidance on the interpretation of this provision, but the wording gives reason to believe that it would also be treated as restricted to allowing a search for and seizure of a particular existing document.

Particularly useful for identifying the authors of racist and other illegal material on Internet is the possibility provided by sec. 2 of the Interception of Communications Act 1985 (Chapter 56 of 1985) to covertly survey messages passing over public telecommunications systems. This requires a warrant issued by the Home Secretary [= Minister of the Interior] inter alia "for the purpose of preventing or detecting serious crime" (subpara. 2(2)(b)). The Home Secretary has power to issue such a warrant whenever "he considers that the warrant is necessary" for that purpose, in the sense that the relevant information is necessary for that purpose and that it could not "reasonably be acquired by other means" (subsec. 2(3)). Unfortunately (from the point of view of law enforcement), the information obtained from such surveillance cannot be used to bring a prosecution against any offendor: the House of Lords held in *R.* v. *Preston et al*[33], that the result of subsecs. 2(2)(b) and 6(3) combined is that information so obtained must be destroyed as soon as the process of detecting crimes has been completed and therefore cannot be used to prosecute crimes. This legislation is accordingly useful for identification of the authors of racist material on Internet, but in order to prosecute the authors, the police will need to proceed, on the basis of the information so obtained, to find independent evidence of the commission of a criminal offence (Refer also to point 2.5, on data protection, below).

32 Source: Detective Chief Superintendent Keith Akerman, Hampshire Constabulary, Chairman of the Computer Crime Working Group of the British Association of Chief Police Officers.

33 [1994] 2 Law Reports, Appeal Cases 130

Switzerland

In a leading decision,[34] the Federal Court recently held that e-mails are covered by the secrecy of telecommunications. It thus upheld the appeal of a technical intermediary (Swiss Online), which refused to disclose the identity of the author of an e-mail.

Swiss Online had refused to comply with the request of a Zurich judge who had requested it to identify the author of an e-mail who sought to extort funds from a private undertaking. This judge, who was responsible for the investigation considered that he was not required to seek the approval of the judge specially designated to lift the secrecy of telecommunications.

The Federal Court took the view that any step in the judicial procedure which sought to identify retroactively the author of an e-mail must have a legal basis and that the approval of the judge specially designated by cantonal procedure to lift the secrecy of telecommunications was essential.

The Federal Court also emphasised the need for legislation in an area which was constantly changing.

2.4. Obstacles in press and media law to holding a person responsible for racist content

In many countries, publications on Internet fall within the scope of application of the national press laws. This classification of Internet content as press or media has important consequences for the investigation of illegal content. On the one hand, the prescription period is very often shorter than that applicable to normal criminal proceedings. On the other hand, the applicability of press laws limits the scope of preventive measures that may be taken against the operators of websites which periodically host illegal contents.

The conditions under which Internet publications will be considered a product of the press are divergent:

Austria

According to a judgement of the *Oberlandesgericht Wien* of 26 November 1997, the Internet is to be counted among the forms of media in the sense of the Act on Media (*Mediengesetz*, the Austrian press law). This decision was subsequently criticised for generally qualifying Internet as a "medium" without examining further requirements such as periodicity of publication or the journalistic processing of content.

Germany

In general, Internet content can be considered as a product of the press if it functionally replaces the print media[35]. To obtain this qualification, particular content has to be processed in a journalistic and editorial manner. The

34 Deliberations of 5 April 2000 in Case 1A.104/1999.

35 Vid. Martin Bulliger, Ordnung oder Freiheit der Multimediadienste, JZ 1996, p. 385, 387.

administrative court of Düsseldorf[36] held that a content provider who gathers information and provides a forum to third parties for their publications does not benefit from the privileges of press law, because the mere fact that the content provider structures and administers the information contained on his web-page is not sufficient to constitute journalistic processing of such content.

In a case concerning the distribution of nazi symbols, the Higher Regional Court of Frankfurt[37] defined the meaning of "publishing" in the context of the Internet. According to the Court, only the first publication of a specific content on the Internet is protected by press laws. If the content (in the pertinent case, a video game wherein nazi symbols were used) is re-distributed by a third person (here, the owner of a mailbox), the this redistribution cannot be considered publication within the meaning of the press laws.

Italy

Courts have implicitly recognized that publications on the Internet, provided they appear periodically, can fall within the scope of press laws[38]. However, most legal commentators are opposed to an assimilation of the Internet to the press[39].

In addition, the consequences of such classification as products of the press vary considerably between the countries examined:

France

The *Cour d'appel de Paris* found that the press laws and in particular the short prescription period of 3 months are applicable. However, the prescription period is not to be calculated in the traditional manner:

> "The civil judgment delivered on 10 July 1997 following the proceedings commenced on 8 April 1997 by the UEJF (Union of Jewish Students of France), states that Jean-Louis Costes relied in his defence, *inter alia*, on the fact that the texts in question had been published on the Internet network on 14 September 1996 and that, consequently, if they did constitute an infringement of the 1881 Act, they could not give rise to criminal proceedings, since the prosecution was already time-barred.
>
> The accused seeks to take advantage of that time-limit, the principle of which is laid down in Article 65 of the Law of 29 July 1881 on the press.
>
> The application of Article 65, which lays down the principle of a three-month period from the first day of publication beyond which the prosecution is barred, has formed the subject-matter of a consistent line of decisions in relation to writing or images disseminated on paper (books, newspapers, posters etc.) or in an audiovisual form (radio, television, cinema etc.) where it is easy to determine the first day on which the

36 VG Düsseldorf, Beschluss vom 25.6.1998, NJW 1999, p. 1987.

37 OLG Frankfurt a.M., Urteil vom 18.3.1998, NSTZ 1999, p. 356.

38 Rome District Court, 6 November 1997.

39 V. Zeno-Zencovich, La pretesa estensione alla telematica del regime della stampa: note critiche, in: Diritto dell'informazione e dell'informatica 1998, p. 15 ss; P. Costanzo, Libertà di manifestazione del pensiero e "pubblicazione" in Internet, ibidem, p. 372 ss; M. Franzoni, La responsabilità del provider, in AIDA 1997, p. 150.

writing or image was made available to the public, if only because it is apparent from the medium itself (newspapers, audiovisual message) or because the time when it was made available to the public corresponds to a specific act (mailing in the case of books).

In order to apply Article 65, it is necessary to determine the date on which the item was first made available to the public, since the principle is thus laid down by the legislature that after three months, in derogation from the general criminal law, the prosecuting authorities and the parties seeking civil damages are no longer authorised to initiate a prosecution in respect of written works, since the disruption of public order deemed to result therefrom or the harm caused to third parties must be regarded as lapsed or made good.

In such a situation the publication results from the renewed intention of the person who places the message on a site and chooses to keep it there or to remove it when he deems it appropriate. The act of publication is therefore continuous. The fact that the offence continues to be committed throughout the relevant period is a concept of positive law in criminal matters and applies to the definition of a number of offences.

The Court therefore finds that by choosing to keep the texts in issue available on his site on the dates on which it has been established that they were there, and in this instance on 10 July 1997, Jean-Louis Costes published them again on that date and ran the risk that the three-month period would begin to run anew from that date".[40]

Belgium

In a recent decision of the First Instance Court of Brussels dated 2 march 2000[41], the Belgian judges followed the French approach in the Costes case. They rejected the argument of the defendant, against whom a preliminary injunction was being sought in connection with a defamation action, that claims arising out of the relevant publication were prescribed. The Court found that "un délit de presse sur Internet doit être considéré comme un délit continu, tant que le texte litigieux reste aisément accessible à toute personne naviguant sur le net à la recherche d'information sur un sujet donné".

Germany

The qualification of Internet content as a press publications would limit police intervention before the publication of an article. This rules is to avoid censorship. The police must wait until content is published before intervening. The seizure of products of the press can only be effected on the basis of a judicial warrant following publication (§§ 97 and 98 StPO). There is no possibility of intervening before publication.

40 Paris Court of Appeal, judgment of 15 December 1999, published on http://www.legalis.net/jnet/

41 Brussels District court, No 2000/77/C on the list of urgent applications, summary and further links available on http://www.juriscom.net

2.5. Obstacles posed by data protection law

In investigating and tracing racist content on the Internet, the law enforcement authorities depend on the access providers' willingness to co-operate. However, their co-operation is very often limited by the laws on data protection. In most States, such laws are rooted in the fundamental right of freedom from interference with private life and therefore constitute a pivotal counter-weight to police investigational efforts.

Germany

Both, the Federal Act on Data Protection and Telecommunications Services (*Teledienstedatenschutzgesetz*[42]) and the Compact of the *Länder* on Media Services (Mediendienststaatsvertrag) contain strict provisions on data protection applicable to Internet which go beyond the general data protection rules and aim particularly at guaranteeing the right to anonymity.

According to these provisions, the use and the collection of fees must be effected anonymously or by using a pseudonym. The establishment of a user profile can only be linked to a pseudonym which makes it impossible to link the user profile to data that would allow the identification of a person. Moreover, the service provider has to guarantee that the client can use the services without being identified by third parties. This provision implements the constitutional guarantee of the inviolability of communications. Data concerning the manner in which clients use the services must be deleted immediately after use, unless longer storage is necessary for billing purposes. Data on the use of Internet services may only be stored, processed or used if this is necessary for modifications of the contractual relations between the service provider and the user, if they are necessary to allow the user to use the Internet, or for billing purposes. In general and subject to narrow exemptions, data obtained for the above mentioned purposes may not be forwarded to third parties unless the user agrees. The Federal Office for the Protection of the Constitution is pressing for the enactment of a provision which would allow data to be passed to the competent law enforcement authorities[43]. However, this proposal has not yet been carried out.

Switzerland

The Federal Data-Protection Officer has no objection to an obligation to keep data on persons who are not suspected of any offence, as a precaution, but considers that keeping such data is a serious breach of personal rights which must be approved by Parliament, in other words it cannot merely be ordered by the Executive.[44]

42 Act of 22 July 1997, BGBl. I, S. 1872

43 Cf. Bericht des Bundesamts für Verfassungsschutz, http://verfassungsschutz.de/publikationen/gesamt/exint06.htm.

44 Report of the activities of the Federal Officer, 1998, p. 236.

United Kingdom

Under both the Data Protection Act 1984 and the revised Data Protection Act 1998, ISPs are generally obliged to respect the confidentiality of "personal data" concerning their customers. That expression would include not only the contents of their e-mail and chat correspondence, but also details of the websites which they visited, the newsgroups to which they posted and so on. An ISP who amasses such information and discloses it to any third party without legal authority is liable to criminal prosecution. Of course, the Acts contain exemptions for the benefit of police operations. Subsec. 28(3) of the 1984 Act and subsec. 29(3) of the 1998 Act both exempt personal data from the normal non-disclosure requirements in so far as the disclosure is made for the purpose of prevention or detection of crime or apprehension or prosecution of offenders and non-disclosure "would be likely to prejudice any of [those] matters ..."

In the result, the Data Protection Acts authorise ISPs to disclose information about their customers to the police where there is a reasonable suspicion of criminal activity, but do not force them to do so. An agreement has been reached between ISPs and the Association of Chief Police Officers, according to which the police will prepare notices in a certain form and containing certain information whenever they wish to obtain personal data concerning the customers of ISPs, but have not obtained warrants authorising them to demand that information. However, ISPs generally respond positively to such notices only in so far as the personal data sought is felt to be of a "non-sensitive" nature[45].

2.6. Problems of international cooperation among police and law enforcement authorities

Sovereign acts of law enforcement authorities can only take place within the national territory. Hence, law enforcement authorities depend on the cooperation of foreign authorities when they want to investigate foreign authors. We know of no attempts by European law enforcement authorities to attack racist material hosted on servers located outside the national territory, other than by asking their own national providers to block access to these sites. International police investigations within Europe are often effected via Interpol or Europol. Although a highly functional forum for police cooperation, Europol is not vested with any particular mandate in respect of Internet crimes. No specific police cooperation modules have been set up exclusively for the Internet. The Council of Europe addressed this problem in its Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology of 11 September 1995:

> "17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignity or international law, an unambigious legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international

45 Source: Detective Chief Superintendent Keith Akerman of the Hampshire Constabulary, Chairman of the Computer Crime Working Group of the British Association of Chief Police Officers.

agreements as to how, when and to what extent such search and seizure should be permitted.

18. Expedited and adequate procedures as well as a system of liaison should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorised to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorised to provide trafficking data related to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented."

In a certain way, the European Union has responded to those needs in adopting its "Legislative resolution embodying Parliament's opinion on the draft Council Resolution on the lawful interception of telecommunications in relation to new technologies[46]". In this resolution, the Council lists the "requirements" to be met in the Member States for the lawful interception of new telecommunications technologies, namely the Internet. The resolution aims at creating common standards for interception, thereby making cooperation between national police forces easier and less bureaucratic.

46 Official Journal C 279 of 1 October 1999, p. 498.

III. THE RESPONSIBILITY OF THE VARIOUS PERSONS INVOLVED IN THE INTERNET

Introduction: The position of the problem

In connection with the fight against racism, in spite of the abundance of racist and revisionist sites, few courts have rules on the questions of liability, whether that of the author of the unlawful contents or that of the technical intermediaries. Several actors come into play: the author of the statement complained of, than the relays, whatever they may be (forum moderators, persons running electronic mailboxes, creators of links), and finally the technical intermediaries, access providers or hosts.

To study the responsibility of these parties is to attempt to determine what law applies in respect of what offences. It must be emphasised here that the problem of liability arises primarily in criminal terms; however, civil actions to have the sites in question closed down, or access to them blocked, are possible.

3.1. Liability of the author

3.1.1. The limits to criminal responsibility: difficulties in identifying the author

As stated in the introduction, the majority of European countries have criminal laws against racist propaganda and there is no doubt that the authors of racist statements must be criminally liable in respect of such statements on the Internet. On the other hand, unlike other means of expression (the press, radio, television), the Internet does not allow the author of a message or a site (what we mean here is the person who made the racist statement, hereinafter "the author") to be clearly identified. Sometimes, in order to make this identification easier, in some countries (France, for example) it is mandatory to make a declaration[47] prior to opening a website. In the absence of such a means of identification, however, how is the author of the offending conduct to be found?

A significant point is that the technical intermediaries are able to keep "log" files, or records of connections, which are of help in identifying the authors of statements circulating on the Internet. Are they obliged to store them, however, and if so how and to whom are these log files to be communicated? The communication of these files must be subject to certain basic conditions and in accordance with well-defined procedures (court proceedings, for example) so that the confidentiality of the information received can be preserved.

By way of illustration, in a French case[48] before a district court the author of racist statements had been found by means of technical channels. This was the first time that a French court had ruled on the dissemination of racist statements on the

47 http://www.csa.fr/html/declar.htm. This site provides all the necessary information concerning a declaration to open a website.

48 The summary of the decision is taken from the site http://www.legalis.net/net/, archives for September 1999. This site regularly places case-law and commentary concerning the Internet on line.

Internet. In this case the author was identified because *access provider lifted anonymity*.

France

On 27 August 1999 a surfer was convicted by the Strasbourg Regional Court (*Tribunal de grande instance*) of incitement to racial hatred and fined FF 10,000, half of this fine being suspended. This individual had expressed racist views on an Infonie discussion group. The management of the access provider had been informed by the person responsible for moderating the discussion groups that a number of unacceptable messages had been posted. The management identified the subscriber corresponding to the IP address of the machine which sent the message and informed the BCRCI (Central Brigade for the Prevention of Computer Crime), which very quickly investigated the matter. Infonie then filed a complaint against a person unknown and agreed to reveal the identity of the subscriber, who admitted the facts.

Another case provides a good illustration of the limits imposed by judicial ignorance of computers; the court had not carried out a more thorough technical investigation, which it rather hastily considered would have been pointless.

France

On 13 November 1998 the Paris Regional Court acquitted Professor Faurisson, who had been charged with placing on line a number of documents entitled *Horned visions of the holocaust*, on the ground that there was insufficient proof of the ownership of the site in question.

Although Professor Faurisson's name appeared on the articles in question, he denied that he was the author or that he had placed them on line. The court observed that the name could have been put there by anyone and that to make comparisons with other documents previously written by Professor Faurisson would be to rely on assumptions rather than on facts.

In substance, the court considered that "since no investigations had been carried out into the operating conditions of the 'AAARGH' site, its relations with the ABBC.Com server and the technical constraints on access to the information, and on altering and disseminating it, for reasons which, moreover, were set out by the prosecutor in his written submissions, it cannot be established that this site is the accessed property and that he alone can use it".

In our view this decision, which states categorically that it is not technically possible to go back to the source, is out of date. A court cannot now rely on the absence of technical investigations to discharge an accused. It is frequently feasible, unless the author has deliberately brushed over the trail by employing caches or mirrors, to go back to the source of the information disseminated to discover its authors.

Belgium

The Belgian court circumvented the technical difficulties of identification and were satisfied with "a convergence of presumption" (the accused was known for his racist views) to convict a surfer (a police officer) who had made racist

statements in a discussion group.[49] No technical investigation had been carried out by the prosecution for the purpose of identifying the TCP/IP address allocated to the computer used by the accused. This address could have been identified with the cooperation of the technical operator, but it was not necessary.

On 22 December 1999 the Brussels Criminal Court (*Tribunal correctionnel*) imposed a suspended sentence of six months' imprisonment on a police officer and former candidate on lists of Vlaams Blok in Brussels-Villes for making racist statements in various discussion groups (contrary to the Law of 30 July 1981 on the prevention of certain acts inspired by racism or xenophobia, as amended by the Law of 12 April 1993).

The accused was also ordered to pay damages of FB 100,000 to the civil party, the Centre for Equal Opportunities and the Fight against Racism.

This problem in identifying the authors of the illegal contents is a matter of concern for certain national parliaments, which have suggested that legislative measures be adopted to enable the person committing an offence to be identified in *criminal* cases.

Belgium

The Belgian Council of Ministers adopted a Bill on computer crime, which was laid before the Chamber of Representatives in October 1999. The Bill provides, *inter alia*, that access providers will be required to identify their subscribers, to trace their communications via their TCP/IP numbers and to keep this information for a period to be determined by a decree.

Switzerland

On 21 December 1999 the National Council (the Lower Chamber) proposed, in the context of the revision of the Law on the Surveillance of Postal Correspondence and Telecommunications, an Article 12 paragraph 3 bis:

"where a punishable offence is committed by means of the Internet, the access provider shall be required to provide the competent authority with any information which will enable the author to be identified".

This provision is currently being examined by the Council of States (the Upper Chamber).[50]

France

On 20, 21 and 22 March 2000 the National Assembly considered the Bill amending Law No 86-1067 of 30 September 1986 on freedom of communication, and on 22 March 2000 it adopted, after its second reading, Article 43-6-4 on the obligation to identify subscribers disseminating contents on the Internet, which concerns not only personal pages but also mailing lists,

49 The judgment and commentaries may be found at: http://www.droittechnologie.org/2.asp?month=1&year=2000

50 See Medialex, 2000, p. 7.

discussion groups and chat rooms. Article 43-6-4 therefore obliges surfers subscribing to a French service-provider to identify themselves to the service-provider and on their sites.

The Law provides that a subscriber who falsely declares his identity is liable to a penalty of six months' imprisonment and a fine of FF 50,000. The same penalty is provided for a host who is unable to reply to a request from the judicial authorities.[51]

Apart from being adopted by the Senate, this Bill must be given a third reading by the National Assembly. It has therefore not been definitively adopted.

3.1.2. Civil responsibility of the "author"

A civil action depends on injury to the individual interests of a person who is able to plead direct harm. The injured party may then request the civil court to bring the offending conduct to an end quickly, notably by using a procedure available in urgent cases, such as the French civil-law interim relief procedure ("*référé*") provided for in Article 809 of the New Code of Civil Procedure. Such a provisional measure is perfectly suited to the world of networks and provides the courts with a flexible and rapid procedure, but it is difficult to implement where racism on the Internet is concerned, because it is not always a simple matter to determine the author of a hateful statement, the victim and the existence of an interference with individual rights.

Italy

The Law on Immigration of 1998 introduced, in Article 35, a new means of combating racism. It makes provision for a *civil* action against racism, so that *any victim* of a racist or merely discriminatory act may request the civil court to adopt any measure necessary to redress it. The court may order that he racist or discriminatory conduct be brought to an end or adopt any measure to put an end to it or to provide compensation for the harm.

In some respects this action resembles the provisional and urgent measures which may be sought to counter actual or potential harm in accordance with the Code of Civil Procedure.

According to the information available, there have not yet been any decisions in which this article has been applied to the Internet.

51 This proposed article led to the defences being raised by the trade organisations both in France (e.g. AFA, the French association of access providers) and abroad. See the commentary by EuroIspa (http://www.euroispa.org): "Ironically, this law may have exactly the opposite effect from its perfectly honourable intentions. It could force French web authors into foreign jurisdictions and make it impossible for French plaintiffs and judges to obtain information on a French web author without recourse to international judiciary cooperation. The message to members of the French Parliament is simple. You should work with ISPs to provide maximum protection for all French citizens, not introduce a law which moves illegal content outside French jurisdiction, hurting French industry in the process."

3.2. Different interveners have different responsibilities

Owing to the difficulties in identifying the authors, and to the procedural obstacles associated with that fact that these authors take refuge abroad, other possible ways of holding others liable for the dissemination of illicit material have been investigated.

3.2.1. The responsibility of the relayers

It will be recalled that by "relayers" we mean an privileged intermediary who facilitates access to offending contents by a link[52], by operating a discussion group or an electronic mailbox. Although he does not control the content, he may make it easier for the surfer to locate sites and guide him in the immense store of information on the web. Does this intermediary risk being held liable, since the creation of the link is ultimately due solely to his initiative? Can he be regarded as appropriating the site or the information associated therewith? The case-law will be described below according to its nature (criminal or civil), and the liability of the relayers is based on the failure to cancel the link.

It should be pointed out at the outset that this heterogeneous and sometimes contradictory case-law does not reveal a clear trend in respect of the responsibility of these intermediaries.

In criminal law there are few examples relating to racist links. The hosts very frequently cut off the links where they are reported to them, in order to avoid proceedings prosecution[53].

> ***Switzerland/link***
> Recently (in March 2000) the personal home page of an assistant lecturer at the Federal Ecole Polytechnique in Zurich was closed down by an internal decision taken by the authorities of the Ecole Polytechnique, acting on their own initiative, because it contained links to racist sites. The matter is currently the subject of an internal administrative and criminal investigation.

The same problem exists in the case of electronic mailboxes. Can those running them be held criminally liable for the messages circulated through them? It seems that they can.

> **Switzerland/mailbox**
> In a decision of 7 December 1998[54] the Obergericht of the Canton of Zurich held that the operator of an electronic mailbox in which

52 On the problems of links, see Droit de l'informatique et des télécommunications 99/3, pp. 6 to 21, *L'utilisation des liens hypertextes, des frames ou des meta-tags sur les sites d'entreprises commerciales*", by C. Curtelin. It is also possible to consult the site: www.jura.ui-tuebingen.de/ and search with the "Stefan Bechtold" search engine. Legal commentary and case-law on hypertext links can then be found

53 See the response of the German Government (Drucksache 13/7757 of 22 May 1997) on the closing of racist sites when the "radikal" case was denounced by the Greens. See, in France, the remarks of alternB, the French host, on website http://www.internet.gouv.fr: joint regulation of the Internet, the position of the trade. "In respect of the 40,000 sites hosted free of charge, I receive an average of one complaint per day by e-mail, one registered letter per month and one judicial complaint every two months. Now, in order to avoid being overwhelmed by procedures, I destroy everything complained of which I consider obviously illegal or contrary to the charter of the service. I am therefore compelled to be judge of the evidence".

54 In Medialex, 2/99 p. 106.

pornographic information was circulated was guilty of a punishable offence within the meaning of Article 197 of the Swiss Criminal Code, since he could have cut off access to that information and had not done so, so that users, in particular minors, could consult it.

A more sensitive issue, on the other hand, is the liability of a participant in an electronic mailbox who merely redistributes information provided by others without "adopting" it.

Germany/box

A German court[55] held that a surfer was not criminally liable on the ground that the unlawful content concerned was not his and that he had not "appropriated" it.

The accused found on the internet in an anonymous mailbox a file called the "Terrorist´s handbook" which contained instructions for building arms. He filed the handbook in the mailbox of another person. This mailbox was accessible to the more then 800 users of an internet club. The accused claimed that he had found the file by coincidence and he admitted that he knew vaguely about the content of the file. In the first instance, he was convicted of giving instructions for the manufacturing of weapons, an offence punishable according to Art. 53 Weapons Act. The Superior Regional Court of Bavaria (Bayrisches Oberstes Landgericht) acquitted the accused in the second instance. According to the Superior Court, it was not clear whether the accused had turned the instructions of the handbook into his own instructions/ had appropriated the instructions of the handbook. The mere distribution of the instructions is not enough to assume such appropriation.

A question which sometimes arises is that of the criminal liability of the various interveners in that special category of sites, chat rooms and discussion groups, owing to their essentially private nature. Antiracist regulations generally specify the precondition that the material in question must be communicated to the public, and this condition is not satisfied in the case of electronic mailboxes or newsgroups. These might at first sight be considered to constitute private correspondence, but the case-law tends to reject that restrictive interpretation of electronic mailboxes.

Germany/public nature of electronic mailboxes

In a case involving an electronic game with Nazi symbols, a German court[56] recognised that a circle of surfers linked to an electronic mailbox was of a public, not a private, nature, even though the circle was restricted.

The accused operated a mailbox in which he had filed a computer game which contained nazi symbols. A small circle of users had access to his mailbox whereby access could be gained anonymously by logging in with a guest login. The accused was convicted for the public use of forbidden symbols (Art. 86a of the German Penal Code). The court made clear that

55 Beyerisches Oberstes Landgericht, Decision of 11 November 1997, NJW 1998, p. 1087.

56 Oberlandesgericht Frankfurt a.M., Decision of 18 March 1998, NSTZ 1999, p. 356.

already the fact of making something optically available constitutes a use. There is no need for the physical supply of the symbol. For the requirement of "public", it is sufficient that the contact to the mailbox can be obtained without identifying the person gaining access. Due to the anonymity of the contact, the group which is using the mailbox is not a circle of private friends but a "public" circle. The place on which the content is filed does not have to be public.

Belgium

In a decision of 22 December 1999 (see 3.1.1) the Brussels Criminal Court considered that "newsgroups" or discussion groups "are places which are not public but open to a certain number of persons". Consequently, they satisfy "the statutory conditions of publicity".

In civil law, maintaining the link complained of constitutes an interference in respect of which an injunction may be issued or an award of damages made.

The Netherlands/link

In a counterfeiting case the District Court, The Hague, held on 9 June 1999 that an access provider was liable for having maintained a link which connected to a site containing counterfeit material[57] :

"Declares it to be the law that by having a link on their computer systems which when activated brings about a reproduction of the works that CST (the plaintiff) has the copyright to on the screen of the user, without the consent of the plaintiffs, the Service Providers are acting unlawfully if and insofar that they have been notified of this, and moreover the correctness of the notification of this fact cannot be reasonably doubted, and the Service Providers have then not proceeded to remove this link from their computer system at the earliest opportunity."

Belgium/link

On 2 November 1999 a Belgian district court held that a technical intermediary was liable for having failed to cut off the offending links and convicted it of aiding and abetting on the basis of the following facts[58] :

Skynet hosts the "somnus" and "freemusic" sites, which offer hyperlinks to sites which allow music recordings to be made in MP3 format. The non-profit-making association ifpi and its member polygram warned Belgacom Skynet sa on two occasions to cut these links. When Belgacom Skynet sa failed to comply with this warning they commenced proceedings for an injunction, claiming that this conduct was contrary to fair commercial practice. The court held that Belgacom Skynet sa could be considered liable since it did not cut the links although it had been informed of suspicious activities. The links in question were conscious links to known pirate websites; Belgacom Skynet sa was therefore guilty of aiding and abetting the offence of making reproductions of music files available to the Belgian public.

57 See details of the case on http://www.juriscom/net/elaw/e-law11.htm

58 A summary of the decision can be found on:
http://www.droit-technologie.org/2_asp?actu_id=1877271291&month=2&year=2000

Belgacom Skynet sa was therefore responsible for the illegal use of copyright material in Belgium and unlawful conduct. In the operative part of the judgment the court ordered Belgacom Skynet to put an end to the practices and to pay a fine in default and ordered that a summary of the judgment be published on the home page of Belgacom Skynet's site and in five newspapers.

Germany : information archiving

In Germany, on the other hand, an archive operator was held not to have civil liability, on the ground that compiling an archive does not constitute adopting a personal position on the content of the information disseminated[59].

The German section of the Church of Unification lodged a civil claim (cease and desist order) against a civil rights institution which published government documents on his homepage that contained affirmations capable of discrediting the Church. The regional court held that maintaining an archive constitutes distribution only in a technical sense whereas an independent contribution to the potentially wrongful act could not be seen in maintaining an archive. The participation in establishing a market of opinions would not be a sufficient ground for civil responsibility. The notification by the claimant about a potentially discrediting content in the defendant's archive does not create civil responsibility.

Italy/newsgroup

On 4 July 1999 the Rome Court dismissed an application for an order for the removal of an advertising message with an allegedly defamatory content which had been published in an "unmoderated" discussion group.

The court held that the forum operator could not be considered personally liable for his activity as operator of the news-server Pantheon srl. Nor did a claim lie against Panthéon (the Internet provider), since the latter merely made available to the users the virtual space necessary to host the forum, and since in this case, which concerned an unmoderated discussion group, had no power to control or monitor the messages placed there[60].

United Kingdom/news group

The Defamation Act was enacted in the United Kingdom in 1996 to protect service provides against unwarranted requests to cut links. The Defamation Act provides that in the case of defamation the technical intermediary will not be liable if it is not the author or publisher of the content in question, if it has taken appropriate measures and if it was not aware of the content in question.

An English citizen complained to Demon (the service-provider) about a message posted in a newsgroup in the United States which defamed him. Since Demon was not the author of the message or the operator of the server of origin it acknowledged the complaint but did not cancel the

59 Landgericht Berlin, 17.3.1998, NJW RR 1998, p. 1634

60 Decision published in: Diritto dell'informazione e dell'informatica 1998, p. 807.

message. Proceedings were therefore initiated against Demon. In a decision of 26 March 2000 the court of first instance, applying the Defamation Act, found that Demon was liable for disseminating defamatory messages in a discussion group and ordered the Internet service-provider Demon to pay damages to the complainant in respect of a content of which Demon was completely unaware.

We conclude this section on relayers by describing a Swedish law, which is significant because Sweden is the only country to have enacted legislation in this sphere and to have clarified liability in an area in which, as we have just seen, the case-law seems to be rather imprecise. This impression of vagueness is accentuated by the sometimes contradictory nature of decisions and the absence of relevant decisions at last instance.

Sweden

This law on electronic mailboxes (original title: *Lag (1998:112) om ansvar för elektroniska anslagstavlor*) originated in 1998. It represents the legislature's response to a line of decisions of the Supreme Court which had exempted the *moderator* of news and chat rooms from any criminal liability[61]. The law imposes on the operator of an electronic mailbox an obligation to exercise diligence under pain of being held criminally liable:

– however, the law applies only to news rooms and chat rooms, in other words to electronic mailing services which allow users to post messages for other users or to see other users' messages; it is not aimed at web sites[62]. Nor does it apply to traditional electronic mail (Article 2 (4)), in other words to messages sent to a specific addressee.

– it exempts purely technical operators from all liability (Article 2) and imposes liability on the moderator (cf. Article 2(1)) of the service, in other words on the person who controls the electronic mailbox and determines what is posted there.

– the management are required to monitor the messages which they make available (article 4); there is no requirement to monitor each new message directly; periodic monitoring will suffice. Where the number of messages is very great and systematic monitoring is difficult the moderator may discharge his obligation by setting up a "complaints message" service which allows users to inform him of unlawful messages[63].

– the moderator is under an obligation to remove messages which are **manifestly** (the management are not required to determine delicate legal questions concerning the scope of the law) illegal, in particular messages that are racist in the sense that they infringe the provision of the Swedish Criminal Code which makes hateful statements an

61 NJA 1996, p. 79.

62 See the commentary by Per Furberg in Karnov CD-ROM, 1999/2000:1, note 1.

63 Furberg in Karnov CD-ROM, 1999/2000:1, note 10.

offence; Article 5(1)(1)) expressly refers to the relevant provision of the Criminal Code (Article 10a, Chapter 16).

– anyone failing to comply with the obligation to remove an offending message is liable to be imprisoned for a minimum of two months, and a maximum of six months in serious cases (Article 7).

3.2.2. The liability of the host

The question is whether this technical intermediary can be held liable where illicit contents are accommodated; whether he will be criminally liable, for example, for aiding and abetting the dissemination of unlawful statements, or whether the rules of civil law will apply, so that liability will be based on failure to observe the code of conduct: failure to prevent the dissemination of such statements.

3.2.2.1. The host: aiding and abetting for the purposes of the criminal law?

Does the fact of providing space for the storage of unlawful information constitute active participation in the offence?

The host is not deemed not to be aware of the content of the information stored and should therefore not be held liable for aiding and abetting. The fact of concluding a simple contract with a customer and making space available for a website or an electronic mailbox should not be treated as conscious participation in offences committed by that customer. The host merely rents space to the customer or grants a sort of lease in a strictly commercial context.

Immediately the host becomes aware that a content is unlawful, however, he could be found guilty of aiding and abetting the offence[64] if he does not take immediate action to prevent its dissemination. Must he therefore assume the role of censor and moral guardian by preventing the dissemination of statements which he deems criminal?

France

In a more or less comparable situation[65] (it did not concern the Internet, but Minitel), the Court of Cassation stated that it appeared impossible to imagine that the director of a server centre hosting a telematic service – which often accommodates a great many services – "is in any way liable for the content of the messages". The Court of Appeal had not convicted the director of aiding and abetting and the Court of Cassation (the highest French court) did not adjudicated on this charge.

64 On aiding and abetting, see the article by Sébastien Canevet, "Fourniture d'accès à l'Internet et responsabilité pénale" (*Provision of access to the Internet and criminal liability*), available at: http://www.canevet.com/doctrine/resp-fai.htm

65 Cass. Crim. 15 November 1990, Bull. No 388.

Switzerland

In Switzerland, on the other hand, a PTT director was convicted of aiding and abetting[66] the publication of obscene material because of the sex chatlines operated by individuals via the telephone networks (and hence accessible by minors). The Federal Court observed that the Attorney General's department had on several occasions drawn the PTT's attention to the possibility that children might listen to or participate in pornographic conversations, and made quite clear that an which provides the instruments necessary for the operation of a criminal service and which, despite being made aware of the criminal conduct, does nothing to stop it is guilty of aiding and abetting the offence[67].

United Kingdom

Part III of the Public Order Act 1986 is drafted in such terms as to conceptually cover the activities of persons who "host" racist material, in the sense of providing the technical platform to allow the author to make it available on internet. In particular, such a host could be said to be publishing or distributing written racist material under subject. 19(1), distributing, showing or playing recordings of racist material under subsec. 21(1) and/or in possession of racist material under subsec. 23(1). The last mentioned provision is particularly relevant, in that it suffices if the material is stored with a view to its being displayed or played later by another person and in that the material need only be shown to be objective likely to stir up racial hatred in the circumstances, not that it was intended by the ISP to be used for that purpose. On the other hand, it is a defence to each of the offences "for an accused ... to prove that he was not aware of the content of the written material or recording, and did not suspect, and had no reason to suspect, that it was threatening, abusive or insulting".

After learning of the German decision of the "Landsgericht München" on the criminal liability of ISPs as accomplices (see below 3.2.3.1), British ISPs asked for clarification of the position under British law. The authorities take the view that, although the Public Order Act was introduced before the proliferation of internet, and although the inclusion of ISPs within its scope is therefore completely fortuitous, ISPs can nevertheless be prosecuted under Part III if they actually know that they are hosting racist material (i.e. it has been drawn to their attention) and they take no action to remove that material[68]. Therefore, no ISP will be prosecuted for unconscious transmission of racist material.

None of these provisions or interpretations thereof have yet been tested in court.

---

66 ATF 121 IV 121

67 "it is irrelevant that he did not intend that the pornographic recordings should be heard by children. He is not charged with having committed the offence as author or co-author. He clearly pursued a different aim, namely the success of mailbox 156; it does not alter the fact that after being informed and given a formal warning by the Vaudois prosecutor, he agreed, by continuing to provide his services, to make a causal contribution to operators who to his knowledge were using this means to commit offences on a regular basis."

68 Sources: Mr. Neil Stevenson, Community Relations Unit, Home Office [= Interior Ministry] and Detective Chief Superintendent Keith Akerman, Hampshire Constabulary, Chairman of the Computer Crime Working Group of the British Association of Chief Police Officers)

3.2.2.2. Civil liability based on the host's misconduct

In addition to the rules on criminal liability, persons involved with the Internet may incur civil responsibility in negligence or for breach of contractual.

A number of decisions[69] seek to recognise that a host is liable in negligence where he has failed to exercise vigilance in respect of the contents which he hosts, in particular where he hosts anonymous sites. This vigilance must only be susceptible of excluding sites which are **obviously** illicit. "Excluding" means closing down the site without delay, where possible after consulting the author of the pages complained of (which is difficult in the case of anonymity).

France

On 10 February 1999 the Paris Court of Appeal, held, on an appeal from an interlocutory decision of 9 June 1998, that a host who allows anonymous persons to create web pages is liable for their content[70].

In the interlocutory order of 9 June 1998 the President of the court had held that "the host is required to ensure that those to whom he provides services observe proper moral standards ... and that they comply with the law and regulations and respect the rights of third parties". Then, "in order to discharge his responsibility, [the host] will therefore have to show that he fulfilled his special obligations to inform the customer of the obligation to respect personality rights, copyright, trade mark rights that he did in fact carry out checks, if need be on the basis of samples, and that when a breach of the rights of third parties was revealed he acted diligently to put an end to that breach..."

The Court of Appeal confirmed the viewpoint of the judge of first instance and maintained the responsibility of the host:

> "... by hosting anonymously on the site altern.org which he has created and which he runs any person who, under any name whatsoever, requests space for the purposes of making available to the public, or to categories thereof, signs or signals, words, images, sounds or messages of any kind which are not in the nature of private correspondence, Valentin Lacambre manifestly exceeds the technical role of a mere conveyor of information and must clearly assume, as against the third parties whose rights are infringed in such circumstances, the consequences of an activity which he has deliberately undertaken to carry out in the conditions referred to above and which, contrary to what he alleges, is profitable and on a scale which he himself claims".

The judgment therefore states that hosting is an activity which goes beyond the mere transmission of data, since it entails the dissemination of the site (a fortiori where that hosting is provided on an anonymous basis) for a fee.

---

69 http://www.droit-technologie.org/2_1.asp ?actu_id=1877271291&month=2&year=2000

70 *Estelle Halliday* v *Valentin Lacambre*, TGI, 9 June 1998 and Paris Court of Appeal, 10 February 1999; in this case Mrs Halliday discovered that 19 photographs showing her completely or partly naked were displayed on a web site and sought an injunction against Mr Lacambre, the host known by the name of *altern.org*

Considered implicitly as a *director of publication*, therefore, the host must assume a certain responsibility where his activity, carried out without prior checks, helps infringe the rights of others.

In this case the liability was civil liability based essentially on wrongful conduct. The judgment refers to a "breach of the right to an image and of the intimacy of private life", and in France the solution is based on a breach of Article 9 of the Civil Code.

This decision was confirmed in a decision of the Nanterre Regional Court of 8 December 1999 which, on the basis of Articles 9 and 1382 of the Civil Code, upheld an action against the host of a website where photographs representing a nude model were displayed.

The court stated on this occasion that a host is under a general obligation to exercise prudence and diligence. He is therefore required to take the necessary precautions to avoid infringing the rights of others. For that purpose, the host must take reasonable steps to provide information. The court considered that the fact that the host drew customers' attention to certain essential obligations when the service contract was concluded, and that there was a "charter" informing customers of the need to respect the rights of others, constituted sufficient diligence.

The host must then show vigilance. This vigilance does not mean the "detailed and thorough monitoring of the content of the hosted sites", but need only be of such a kind as to exclude sites whose "unlawful nature" is "obvious". Finally, the host ensure that he has the facilities to close down dubious sites immediately and ensure that they are not reopened. For the remainder, the judgment contains an important dictum. The fact that the host is unable to provide the identity of the person who created the site in issue does not in any way exempt him from liability. The Regional Court considered that the activity of a host "by virtue of its nature and the conditions in which it is carried out ... gives rise to liability".

The liability of the host has just been established in a case concerning domain names[71]. Archives of February 2000, see text of decision and commentary. What should be particularly emphasised in that judgment is the joint and several liability of the actors: the person registering the domain names, the person organising their sale and the host.

Thus the auctioning on the Internet of domain names reproducing well-known brands (les-3suisses.com, la-redoute.net) constituted an act of forgery and "reveale[d] a parasitical intent". In the court's view the person who had registered the domain names, the person who had organised the sale and also the host of the site on which the sale took place were all liable.

As regards racism, the Nanterre Regional Court is shortly due to determine a case involving Nazi sites[72]:

71 Interim order of the Nanterre Regional Court 31 January 2000 http://www.legalis.net/jnet/

72 Links relating to the article: http://www.multimedia.fr http://www.uejf.org

On 18 February 2000 Multimania (a host) removed a Nazi site from its servers at the request of the UEJF (Union of Jewish Students of France). Called "nsdap", like the Nazi party, the site posted pages glorifying the Third Reich, contrary to the Multimania users' charter. Even though Multimania had removed the Nazi site, the UEJF decided to bring *civil* proceedings in negligence against it.

The UEJF relied on Article 1383 of the Civil Code, which provides that everyone is responsible for his own actions, his omissions and his imprudence. Its counsel maintained that Multimania had been negligent in failing to monitor the content of the site in question and in delaying removing it from its servers. The UEJF claimed damages of one franc and an order that the defendant should set up a security procedure to be followed when new accounts were opened. It is apparent that access to the Multimania host service is not subject to any condition relating to identity.

The UEJF is not seeking police-type control, but its counsel argued that "a host cannot be satisfied with the identity provided by subscribers, but must endeavour to know with whom he is contracting. Some hosts require at least the e-mail address of the person, which proves that he has at least registered with an access provider".

Counsel for the UEJF stated that: "Today we ask Multimania to establish a security procedure and to carry out a minimum control of the content of its sites. It could, for example, develop a search procedure based on simple key words, which would enable a considerable number of items to be detected. The intention is that Multimania should be under an obligation to produce results. Furthermore, I [counsel for the UEJF] am in contact with counsel for the other side and am prepared not to proceed with the complaint before the court if Multimania establishes measures in the meantime".

The UEJF has also lodged a *criminal* complaint against the authors of the Nazi site, even though their identity is unknown.

On 24 May 2000, the High Court in Nanterre passed down its judgement in this case. The anonymous author had been identified through the application of the usual rules of judicial procedure, and the Court did not deem that Multimania was in any way to be held responsible, considering that the host provider had respected its general obligation to exercise due caution and diligence.

The Court considered that carrying out a search for precise key words could require "a specialised culture which the host provider cannot be held responsible for not possessing", and, recognising that the profession was also subject to human limitations, called for a sharing of knowledge and experience between organisations devoted to combating incitation to racial hatred and Internet providers.

Likewise, in its judgement of 8 June 2000, the Court of Appeal of Versailles struck down the first-instance judgement passed by the Nanterre High Court on 8 December 1999 in the case between Mrs Lacoste and the Multimania

company. The Court of Appeal noted that "the obligation incumbent on the host provider to exercise due caution and vigilance as regards the sites which it hosts is an 'obligation of means'" and "does not imply a general and systematic examination of the contents of the sites which it hosts".

Italy

A judge[73] found that an author was liable in respect of defamatory statements and made an interlocutory order that the interference be brought to an end. This decision leaves open the question of any liability on the part of the technical intermediary, although it points out that in this case liability was excluded by the contract.

According to another decision, however, a technical intermediary who merely provides access to the network and space on its server for the publication of information services by the provider of information is not liable for any breach of copyright by the latter[74].

This part on the liability of the host may be summarised as follows:

1. ***The host is not automatically and systematically liable in respect of the illicit contents hosted.***

2. ***However, judicial decisions tend to find liability (civil or criminal) on the part of the host where the latter is aware of the contents in issue.***

3. ***In addition, certain countries (France, in particular) mean to impose an obligation on the host to exercise diligence which requires him to show that he censors the information which he accommodates.***

3.2.3. The liability of the access

3.2.3.1. Liability of the access provider for aiding and abetting offences

As a simple intermediary between user and host, the access provider is in principle unable to check the millions of items of information which circulate on the network and are frequently altered. He should therefore *not be held criminally liable* unless the mental element of the offence can be established, since he merely provides a *simple connection service*.

In order to be guilty of aiding and abetting, the access provider must therefore have actually participated in the criminal act and there must be a link of causality between the activity of the accomplice and the commission of the offence by its author. It should also be shown that the access provider intended to participate in the offence.

73 Order of the President of the Teramo District Court, 11 December 1997.

74 Cuneo District Court, 23 June 1997, in *Giurisprudenza piemontese* 1997, p. 493.

A number of theoretical questions arise: can the provision of access to the Internet be seen as actual participation in the offence such as to render the access provider liable for aiding and abetting? Can the access provider's intent to participate be established merely from the act that he disseminates documents of whose unlawful character he is not aware? The access provider cannot be expected to examine all the information which he disseminates and determine whether it is lawful. The essential issue is whether an access provider who becomes aware that illicit information is circulating by means of the facilities which he provides has the technical and legal resources actually to prevent the unlawful information from being received on the *local* network which he controls. He has two options: he can either block access to the information or filter the information to ensure that it cannot be consulted, and both of these operations are aimed **solely** at the surfers on the network which he controls.

It must be emphasised that the access provider has no means of taking action in respect of a server situated abroad which hosts the illicit contents.

A German decision[75] answered some of these questions by clearing the access provider:

> ***Germany***
> By judgment of 8 December 1999 the Landgericht, Munich acquitted the director of CompuServe GmbH, Felix Somm, of providing access to paedophile contents.
>
> Mr Somm was charged with facilitating consultation of paedophile newsgroups (of the "alt.sex.pedophilia" type) by providing access to the news server of CompuServe Inc. In spite of the fact that these news groups were hosted in the United States by CompuServe Inc., he was convicted at first instance by judgment of the Amtgericht Munich of 28 May 1998 and given a suspended sentence of two years' imprisonment.
>
> The Landgericht set aside the judgment delivered at first instance and confirmed the principle that access providers are not liable for the illicit content to which they provide access.
>
> This principle was already established in the legislation in force in a number of countries (in particular Article 5(3) of the German Teledienstegesetz of 13 June 1997 and Section 512(a) of the United States Digital Millennium Copyright Act of 28 October 1998) and in an international convention (cf. the Joint Declaration concerning Article 8 of the WIPO Treaty on copyright of 20 December 1996) and in the amended proposal for the European Directive on certain legal aspects of electronic commerce of 1 September 1999 (Article 12).

75 The French summary which follows is taken from website: http://www.droit-technologie.org/2_asp?actu_id=1475345633&month=1&year=2000

The facts of the case were as follows:

The American company CompuServe Inc. hosted on its news server a number of news groups with a paedophile content; the German company CompuServe Information Services GmbH allowed German subscribers to access these news groups at reduced connection fees; CompuServe Inc. was the only company with contractual links with the German subscribers; following a search (on 22 November 1995) the German State Attorney's Office informed Mr Somm of the existence of the illicit news groups and sent him an initial list of five illicit news groups; since CompuServe GmbH did not have the technical means to cut off access to the news groups, Mr Somm immediately sent the first list to CompuServe Inc. and asked it to cancel the offending news groups; on 29 November 1995 the State Attorney's Office established that these news groups were no longer accessible; on 8 December 1995 a second list of 282 paedophile news groups was sent to Mr Somm; Mr Somm again immediately forwarded the list to CompuServe Inc. and asked it to cut of access to these news groups; between 22 December 1995 and 13 February 1996 CompuServe Inc. cancelled access to the majority of these news groups; on 16 February 1996 CompuServe Inc. informed the press that it considered it was no longer required to intervene, since CompuServe Inc. and CompuServe GmbH now made available to their customers a control tool called "Cyber Patrol-Parental Control", also available in German, which allowed subscribers themselves to censor access to the news groups of their choice; since then new unlawful news groups had been accessible and proceedings had been initiated against Mr Somm.

On the thorny issue of aiding and abetting, the Landgericht decided that Mr Somm had not aided and abetted the offences. It took the view that this offence was conditional upon proof of misconduct on Mr Somm's part and that in the instant case such misconduct could only result from the two following omissions:

The fact that Mr Somm had not reiterated his request to CompuServe Inc. to cut off access to the news groups in question was irrelevant. On this point, the Landgericht considered that such a step had no prospect of success, in view of the contrary official position (in the press) adopted by CompuServe Inc. Mr Somm was therefore not guilty of misconduct by failing to pursue the matter with the parent company.

The Landgericht also considered that Mr Somm should be acquitted pursuant to Article 5(3) of the German Teledienstegesetz of 13 June 1997, which provides:

> "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".

The crucial point is therefore the access provider's knowledge of the illicit content of the information conveyed through his intermediary; this knowledge is held to be culpable if nothing is done to put an end to the interference.

Switzerland

The Federal Court has not yet had the opportunity to rule directly on the criminal liability of access providers in respect of the content of the information which they transmit.

However, legal commentators, and a group of experts from the Federal Justice Office, have taken the view that the decision which established that the PTT manager was liable (cf. 3.2.2 above) could be applied by analogy to access providers[76]. Access providers could be held accountable for the illicit publications which they convey through their access points. In its legal opinion of 24 December 1999[77], moreover, the Federal Justice Office concludes that even simple access providers might be liable as accessories if the author could not be prosecuted (Articles 22 and 322 bis of the Criminal Code)[78]. Owing to the distance between provider and author, criminal liability could only be considered within narrow limits; it would mean, in particular, that the access providers had been made clearly aware of the illegal content by a criminal prosecuting authority.

3.2.3.2. *Access providers and civil liability*

The essential function of the access provider is that of provider of technical services, responsible for connecting its subscribers with sites or other users. In the case of a purely technical activity, an access provider should incur civil liability only where he is aware of or able to control the information complained of.

France

On 15 March 1996 the Union of Jewish Students of France (UEJF)[79] lodged an application for interim measures against nine French Internet access providers (Calvacom, Eunet, Axone, Oléane, CompuServe, Francenet, Internetway, GIP

76 Report of the group of experts cited, p. 9. See also I. Cherpillod, *Quelques problèmes juridiques liés à Internet* (Legal problems associated with the Internet), Plädoyer, 1997 p. 42.

77 See http://www.bj.admin.ch/themen/ri-ir/access/intro-f.htm for the link in French.

78 *Article 27 of the Criminal Code*

1. Where an offence has been committed and perpetrated in the form of publication by one of the media, the author alone shall be liable, subject to the following provisions.
2. Where the identity of the author cannot be discovered or where he cannot be brought before a court in Switzerland, the editor responsible shall be liable, pursuant to Article 322 bis. Where there is no editor the person responsible for the publication in question shall be liable, pursuant to the same article.
3. Where the item concerned was published without the author's knowledge or against his wishes the editor or, in the absence of an editor, the person responsible for the publication shall be liable as the author of the offence.
4. The author of an authentic account of public debates or official statements of an authority shall not be liable to any penalty.

Article 322 bis of the Criminal Code

The person responsible within the meaning of Article 27(2) or (3) for a publication constituting an offence shall be liable to a term of imprisonment or a fine if he deliberately did not oppose publication. Where he acted negligently he shall be liable to a short term of imprisonment or a fine.

79 Paris Regional Court, 12 June 1996, Réf. 53061/96

Renater and Imaginet) on the ground that these service providers were allowing their customers to access negationist servers and messages. The UEJF requested the court to order the respondents to prevent their customers from accessing messages and servers which did not comply with Article 24 bis of the Law of 1881 (as amended by the Law of 13 July 1990), and to pay a fine if they failed to comply with the order.

The court made an interim order on 12 June 1996 and, taking note of various ethical commitments given by some of the parties, rejected the UEJF's application, on the ground that:

> "... an access provider under no legal obligation to regulate the information available on the network, whether this information can be consulted by its customers or whether it is transmitted by them, since the authors alone are liable in respect of such information".

In a court decision of 22 May 2000, the French legal system enjoined the American access provider Yahoo! to take measures to "make it impossible" for French Internet users to gain access to its auction site offering Nazi objects for sale. The judge of the magistrates' court in Paris, sitting in chambers to deal with matters of special urgency (*juge des référés*), gave Yahoo! a deadline of 2 months to present technical proposals as to how the problem might be resolved, commenting that this auction was an "insult to the collective memory" of France.

The Californian company Yahoo! Inc was brought before the courts by the *Ligue internationale contre le racisme et l'antisémitisme* (Licra) and the French Union of Jewish Students (UEJF). These two associations requested at the hearing of 15 May 2000 that "the necessary measures be taken to prevent, throughout the whole of the French territory, the exhibition and sale on this site of Nazi objects."

The judge was of the opinion that "in allowing this site to be viewed in France, Yahoo! is committing a offence on French territory, even if this was not the intention." "Yahoo! is in a position to identify the origin of calls, which should allow it to deny French Internet users access to view this site", the judge concluded.

To summarise this section on the access provider: owing to its essentially technical functions, an access provider should not bear civil or criminal liability unless he is aware of and able to block access to the illicit contents.

3.3. Legislative solutions and measures in the process of preparation

3.3.1. Legislation

Two countries, Germany and Austria, have enacted legislation on the liability of technical intermediaries. These legislative approaches are favourable to a purely technical intermediary and preclude any provision for automatic liability; instead,

they prefer liability to be established *a posteriori*, on a case-by-case basis, depending on knowledge of the content and the means of controlling it.

Germany

Following the judgment at first instance concerning CompuServe, Germany legislated by promulgating the law on information and communications services (Informations- und Kommunikationsdienste-Gesetz)[80] of 22 July 1997, thus generally defining the liability of a service provider for illegal contents. According to paragraph 5 of that law, liability is on a graduated scale and depends on the extent of knowledge of the illegal content:

"§ 5: Responsibility

(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.

(4) The obligations in accordance with general laws to block the use of illegal content shall remain unaffected if the provider obtains knowledge of such content while complying with telecommunications secrecy under § 85 of the Telecommunications Act (Telekommunikationsgesetz) and if blocking is technically feasible and can reasonably be expected."

The distinction which German law draws between the various functions of the provider is similar to the Anglo-Saxon distinction between access provider and content provider. The provider may be a mere technical intermediary whose sole function is to provide access to information on the web.

The provider may also be the person who "uses" foreign contents and processes foreign information in any way whatsoever.

Thus a "provider" who merely conveys the contents is not responsible for them (3)

A provider is jointly liable in respect of illicit contents where he is aware of them, if he is technically able to block them and can reasonably be expected to do so (2).

A provider is fully liable in respect of contents of which he himself is the author. The illegality of the content is determined according to criminal law.

80 BGBl. I p. 1870, in force since 1 August 1997.

However, a provider is under no general duty to carry out a *preventive* control of the content accessible to his customers.

Austria

Similarly, Austria has provided, in Article 75 of the Law on Telecommunications[81], that an access provider is not liable[82] as a technical intermediary. However, an access provider can be reasonably expected to block access to sites whose content he knows to be illegal, and he himself will incur criminal responsibility if he fails to do so.

Because of his function, the "service provider" runs the same risk. He can be expected to employ out reasonable monitoring procedures in the form of specific controls which are not beyond his financial means. He is not held liable if he can show that he followed these procedures; but he will be held liable if it can be shown that he did not effect any control.

Italy

The only rule to refer to the "telematic" dissemination of illicit contents is Article 3 of Law No 269 of 3 August 1998 on the sexual exploitation of minors (which provides that anyone who "by any means, including by telematic means, distributes, disseminates or makes public pornographic material or distributes or disseminates messages or information fro the purpose of attracting or sexually exploiting persons under the age of 18 years" is guilty of an offence). This provision is drafted in very broad terms and might be interpreted as extending liability to all technical intermediaries. It has attracted much criticism for that reason; a Bill providing that the distribution of pornographic material concerning minors is an offence only if it is done "consciously" was filed at the Senate on 14 January 1999.

3.3.2. Measures in the process of preparation

France

In France an initial Bill[83] provided that companies operating host websites would not be liable unless "they themselves have contributed to creating or producing the offending content" or if "after being ordered to do so by a judicial authority they have failed to take prompt action to prevent access to this content, provided condition that they store it directly". This text introduced by the National Assembly dealt with civil liability.

However, the Senate opted for quite a different solution, involving *criminal liability*. The text adopted by the Senate extended the cases in which access providers are liable. Thus they may be prosecuted if they have participated in

81 Telekommunikationsgesetz, BGBI. 1997/100

82 See *Die Haftung des Providers*, *Arbeitsunterlage und Diskussionsgrundlage für de ISPA-Sitzung vom 13. Oktober 1998*, p. 7 *et seq.*

83 On a proposal from Deputy P. Bloche. The French Parliament is currently examining a Bill amending the Law of 1986 on freedom of communications, certain provisions of which allow the conditions under which technical intermediaries on the Internet will be liable.

creating or publishing the illicit contents or if they are initially responsible for transmitting the contents or for making them available.

They may also face prosecution if they refuse to reveal the identity of the authors of publishers of these contents to "third parties who show that they have a legitimate interest".

A further innovation is that the Senators imposed an obligation to exercise diligence "to recognise and not to interfere with the technical measures put in place by owners of intellectual property rights to enable the works or recordings transmitted to be identified or protected".

Following a second reading the National Assembly on 22 March adopted Article 1A of the Bill on audiovisual media concerning the liability of Internet access providers or hosts. It sets out three cases where these service-providers may be liable in respect of the content and not merely in respect of the content and not merely for the breaches of the rights of others resulting from the content:

1. They may face prosecution if they have contributed to the creation or production of the documents in issue.

2. They will also risk prosecution if they have failed to take prompt action to prevent access when ordered to do so by a judicial authority.

3. Finally, these service providers will be liable if "they have been notified by a third party who considers that the content which they host directly and permanently is illicit and harmful to that person and have failed to act with due diligence".

In the course of the debate it was stated that "appropriate measures" meant bringing the matter before a judge, by application for an interim order or by the normal procedure, and forwarding the complaints received to author of the content so that he could alter it.

Unless the Senate adopts this text in the same terms, it will have to be given a third reading before the National Assembly before a final vote is taken.

Finally, after several debates, the French National Assembly adopted on 16 June 2000 a draft law on freedom of communication to amend the law of 30 September 1986. According to this law, host providers or editors**,** whether their services be free or fee-based, will in future be held responsible under criminal and civil law for site contents if, after being approached by the judicial authorities, they fail to put in place appropriate measures to prevent access to the sites in question. They will also be held responsible if, after being approached by a third party who considers that the contents they host are illegal or prejudicial to that third party, they have not carried out the appropriate checks.

Belgium

In an opinion of 28 March 1997 the Supreme Council for Audiovisual Media of the French Community expressed its preference for liability in accordance with the general law rather than cascade liability. By way of example, the Council considered "that an access provider who cannot exercise any a priori control over the Internet resources should not be concerned by the fact that he has omitted to exercise such a control"[84].

3.3.3. The particular case of the European Union and the United States

3.3.3.1. The European Union

In view of the commercial stakes associated with the Internet, the European Union is currently considering a proposal for a directive on certain legal aspects of the services of the information society, and in particular electronic commerce, in the internal market[85]. The proposed directive seeks to establish a legal framework to ensure the free movement of the services of the information society between Member States, but not to harmonise the sphere of criminal law as such.

In the case of host services (Article 14), the proposed directive establishes an exemption from liability for a service provider who stores information, provided that:

> "... the provider does not have actual knowledge that the activity or the information is illegal" or
> " ... the provider, upon obtaining such knowledge, acts expeditiously to remove or to disable access to the information".

In Article 15 the directive proposes that providers should be under no general obligation to monitor the information concerned.

The directive is at present being debated.

3.3.3.2. Les Etats-Unis: Liability of Internet Service Providers (ISP's) and Internet Access Providers (IAP's)

Prior to the adoption of the Communications Decency Act ("CDA") the development of American case law had led to a seemingly paradoxical situation concerning the liability of providers. Where the provider exercised little or no editorial control over the content it provided, the provider would not be liable unless it knew or had reason to know that such content was defamatory[86] whereas a provider who exercised such control would be acting as a publisher and, as such, would be liable for any defamatory content[87]. An operator which assumed responsibility for at least attempting to keep defamatory or offensive material from being posted was liable

---

84 Opinion referred to in the Report of the French Council of State, *The internet and numerical networks*, 1998, p. 111.

85 See the common osition adopted by the Council with a view to adopting a Directive of the European Parliament and the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce"), 14263/1/99 REV 1.

86 Walter Pincus, "The Internet Paradox Libel, Slander & the First Amendment in Cyberspace", 2 Green Bag 2d 279 (Spring 1999), discussing Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

87 Stratton-Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y.Sup. 1995).

as a publisher for defamatory postings, but an operator which made no such attempt escaped publisher liability[88].

In order to encourage self-regulation within the industry, Congress specifically addressed this situation in the CDA by exempting access providers from liability for providing access or connection to or from a facility, network or system not under their control[89] and providing that service providers may not be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be objectionable, whether or not such material is constitutionally protected[90]. Although other sections of the CDA have been declared unconstitutional, provider defences to liability remain in force and courts have interpreted these sections to provide broad immunity to providers.[91]

This immunity is not unlimited in all areas. With respect to copyright and trademark rights, the Digital Millenium Copyright Act prescribes specific actions that an Internet provider must take, after it has been informed of a possible copyright infringement being carried on its service, in order to avoid liability. Unlike in defamation cases, the requirement of monitoring content is deemed to be bearable in this context.[92]

3.4. Laws on the press/criminal responsibility

The press is generally governed by its own legal regime, especially in respect of liability for the editorial content. Liability is exclusive, the idea being that only one person is to be held responsible[93]. The question therefore arises whether these laws on the press and the particular types of liability which they establish also apply to services offered by the Internet other than private correspondence services (e-mail).

Italy

Criminal law on the press :

Articles 57 and 57 bis of the Criminal Code govern criminal liability for offences committed by means of the press. In the case of the periodical press, the editor or deputy editor is liable if he has failed to monitor the periodical sufficiently to prevent the commission of offences. The penalty is that laid down for the offence in question, reduced by one third (Article 57). In the case of the non-periodical press, the law provides, in the same conditions as Article 57, that the publisher is liable, or the printer if the publisher is not indicated (Article 57 bis).

---

88 Pincus, *op. cit.* at 282, quoting Douglas B. Luftmann, "Defamation Liability for On-Line Services: The Sky Is Not Falling", 65 Geo. Wash. L. Rev. 1071 (1997).

89 47 U.S.C.§223(e).

90 47 U.S.C. §230. This is sometime referred to as the "good samaritain defense".

91 Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997)cert. denied, 425 U.S. 937 (1998) (AOL not liable for failure to remove defamatory messages after repeated requests of victim); Blumentahl v. Drudge, 992 F.Supp.44 (D.D.C. 1998) (AOL not liable for contents of paper it paid author to produce); Doe v. America Online, Inc., 718 So.2d. 385 (Fla Ct. App 4th Dist. 1998) review granted 729 So.2d. 390 (Fla. Sup. Ct. 1999) (CDA pre-empted state statutes and shields AOL from liability for sale by one of its members of child pornography through a "chat room" despite notice to AOL of such sales).

92 Pincus, *op.cit* at 287.

93 See D. Barrelet, *Droit de la communication*, Berne, 1998, p. 330. The author explains the origins of this special liability known as cascade liability, formerly envisaged as a way of allowing the publication of anonymous articles and avoiding lengthy and complicated proceedings.

The question therefore arises as to whether these provisions can be applied to publications on the Internet and, if so, who is liable. There are no criminal decisions on this point. Thus far, however, legal commentators refuse to treat the Internet in the same way as the press[94].

France

A number of existing laws apply to the press: the Law of 1881 on the freedom of the press, which is now applicable to "all audiovisual communications media"[95] and the Law of 1986 on freedom of communication[96]. Although these laws do not refer expressly to the Internet, the courts have not been slow to classify the Internet as audiovisual communication and to apply the provisions on liability to it[97].

French law has established cascade liability: in the event of a press offence[98], proceedings are first brought against the editor and, in the alternative, the author and then the producer.

Legal commentators and case-law are divided as to whether this liability should be applied to the Internet. Thus in its report concerning the Internet[99] the French Council of State accepted that

> "editorial liability should be maintained in respect of relevant matters, i.e. the publication of the contents, but a system of *liability in accordance with the general law* should be retained for all other functions exercised on the network and in particular the functions of technical intermediation or website design".

The French courts do not appear to have followed the line recommended by the Council of State, however. Thus the Criminal Chamber of the Court of Cassation delivered a judgment on 8 December 1998 in which it relied on Articles 92-2 and 93-3 of the Law of 29 July 1982 on audiovisual communications and held that the person described as the producer bore *criminal* liability. The person in question had opened a telematic service "36-15 Renouveau", a veritable discussion group, and had then been prosecuted

---

94 None the less, in a decision in civil proceedings (unfair competition) the owner of an Internet domain name was assimilated to the proprietor of a newspaper (or a radio or television station) and held to be under an obligation to exercise diligence and, consequently, to be have direct civil liability: Naples District Court, 8 August 1997, published in *Diritto dell'informazione e dell'informatica*, 1997, p. 970, and in *Giustizia Civile*, 1998, p. 259. The owner of a domain name is therefore liable in civil law for unlawful acts committed as a result of the content of pages placed on the site which he operates ; he is under an obligation to check diligently whether the distinguishing mark belongs to the person inserting the relevant pages and to monitor the content of the message in order to ensure that the advertisement is clear, truthful and accurate. This principle applies even where the owner of the domain name is only involved with the technical maintenance of the site and the creation and management of the pages placed on the network, and the associated commercial negotiations, are entrusted to another person.

95 According to the legislative amendments introduced by Law No 85-1317 of 13 December 1985.

96 Law No 86-1067 of 30 December 1986 "on freedom of communication", *Journal Officiel*, 1 October 1986, p. 11511.

97 Article 93.3 of the Law of 13 December 1985 defines the conditions for the application of editorial liability in audiovisual matters. The offending message must have been the subject of a declaratory judgment before it was communicated to the public. Liability is borne primarily by the editor of the publication, then by the author and finally by the publisher.

98 The press offences already determined by the Law of 29 July 1881 (Article 23 *et seq.*) were, in particular: incitement to commit felonies and misdemeanours; incitement of discrimination, hatred or racial violence; personal offences (defamation, insults).

99 *Internet et les réseaux numériques*, Report of the Council of State, 1998, is available on the following site: http://www.Ladocfrancaise.gouv.fr

after two anonymous (racist) messages had been disseminated on this site. The lower courts had acquitted him on the ground that since he had no control over the messages disseminated he could not be regarded as the producer. However, the Court of Cassation considered that by taking the initiative to see up an audiovisual communications service for the purpose of exchanging political opinions, the accused knew beforehand what themes which would be dealt with, he actually stored the information found there and was required to ensure that the statements did go beyond the context of the forum. He could therefore be prosecuted as producer without being able to plead that he had no knowledge of the contents.

> "... having taken the initiative to set up an audiovisual communications service for the purpose of exchanging opinions on pre-defined themes, Mr R. could be prosecuted in his capacity as producer and could not plead in his defence that he had not monitored the offending messages."

This judgment is an interesting application of cascade liability in respect of a telematic service.

However, the question whether a *host*, whose role is more remote and who has no influence over the content of the offending site, may be held liable in respect of its content remains open.

As regards the *access provider*, the Puteaux District Court held in a decision of 28 September 1999 that "the director of an audiovisual communications service is the person who can exercise control *before* publication, the person who has control of the content of the service", and held that the access provider did not have editorial responsibility.

Finally, in a specific case involving dissemination of racist statements, the Paris Court of Appeal, in a judgment of 15 December 1999, applied the Law of 1881 on the press and held that changing of the address of an Internet site is an act constituting "a fresh publication" within the meaning of the Law of 1881 on the Press. Accordingly, the three-month period provided for in Article 65 of the Law of 1881 after which the prosecution of offences committed by means of the press becomes time-barred begins to run from the date of the change of address. The fact that the content of the site at the new address is the same as that at the original address does not mean that the prosecution is to be regarded as time-barred[100].

The specific function of the Internet based on the vast amount of information accessible via hypertext links is a function based not on control of the content but on an increased ability to consult and access it. This network is therefore far removed from the classic publication of contents and makes it difficult to establish a single regime of liability based on the cascade principle.

100 Moreover, at first instance the court had taken the view that "the publication results from the renewed intention of the person transmitting it, who places the message on a site and chooses to keep it there or to remove it when he pleases. The act of publication is therefore continuous".

Switzerland /liability by default

The recent revision of the criminal law on the media, which entered into force on 1 April 1998, has *limited the subsidiary responsibility* (based on Article 322 bis of the Criminal Code, see 3.2.3.1, note 78, above, which raises the intentional element of the offence) of the network operator in the sole case where liability cannot be attributed to another person, in particular because the author of the publication cannot be discovered or is abroad[101]. This may pave the way for liability "by default" for access providers but gives rise to a certain amount of *controversy*[102].

However, this point of view may be tempered where racist matters are concerned. In a recent decision concerning a book shop guilty of having disseminated works of a racist nature, the Federal Court[103] refused to give the accused the benefit of Article 27 of the Criminal Code because the application of such a provision would produce a result contrary to the aim pursued by the law.

> "Where a criminal provision is designed to prevent the publication of certain statements or to prohibit illicit publications, to allow those responsible for such publications to benefit from a special arrangement would amount to deviating from the aim pursued by the legislature".

In this case the Swiss retailer of certain racist and revisionist works, whose known author (R. Garaudy) had already been convicted abroad in respect of the same publications, was acquitted at first instance of the charge of disseminating racist and revisionist statements in application of Article 27, in accordance with the following reasoning: since the author of the book had already been convicted, all those assuming only subsidiary responsibility to that of the author should avoid punishment, a fortiori a retailer, even though there was no specific reference to retailers in Article 27 of the Criminal code.

The Federal Court rejected that argument, annulled the decision and remitted the case to the cantonal court. It delivered what in our view is a rather political decision which might be seen as a warning to potential disseminators of racist material: Article 27 of the Criminal Code will not allow a hateful statement to be spread with impunity.

Returning to the problem of the Internet, criminal law on the media (Article 27 of the Criminal Code and liability responsibility by default) is therefore not applicable in the case of racial discrimination, hard pornography and the depiction of violence. According to the legal opinion of the Federal Office of Justice referred to above, the situation existing before the entry into force of the criminal law on the media prevails: access providers could therefore be punished for *aiding and abetting* the main offence.

---

101. Government explanatory report concerning its proposal to revise the criminal law on the media, *Feuille Fédérale* 1996 IV, p. 560.

102 J.P. Müller, op. cit., p. 203.

103 ATF 125 IV 206

It emerges from these cases that the transposition of the laws on the press and the media, together with their privileges and special features, to the Internet is in our view inadequate in the light of the number of actors involved on the web and the lack of clarity as to their role. If cascade liability should be envisaged, there should be specific provisions to that effect and the task of each of the persons involved and the liability associated with those tasks should be clearly defined.

IV. THE POSITION UNDER PUBLIC INTERNATIONAL LAW

The duties of States under public international law in respect of the dissemination of racial hatred through the Internet are not yet clearly established. Only one binding multilateral treaty deals expressly with the dissemination of racist doctrines and incitement to racist violence and none deal expressly with revisionism or racism on the Internet. The practice of States in this respect is not uniform and there is considerable dissension among the representatives of States and other expert jurists as to the measures which States are obliged to adopt in order to combat such expressions of racism.

4.1. Texts which enunciate legal duties

The obligation incumbent upon all States to prevent and prohibit discrimination on the basis of race is enshrined in Arts. 55(c) and 56 of the Charter of the United Nations and has been subsequently reiterated in numerous multilateral conventions[104]. A duty of States in respect of racist propaganda is implied by the Universal Declaration of Human Rights, which declares in its Art. 7 that all human beings are entitled to the equal protection of the law against any incitement to discrimination. The concrete obligations of States in this respect are set out in Art. 4 of the International Convention on the Elimination of all Forms of Racial Discrimination (ICERD). As this is the only binding norm which potentially obliges all States to introduce legal norms prohibiting and punishing the dissemination of racist material, it is worth quoting in relevant part:

> "States Parties ... undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, [racial] discrimination and, to this end, with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention, *inter alia:*
>
> (a) Shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or

104 Some prohibit racial discrimination either generally, or in respect of all of the exercise and enjoyment of all of the rights enunciated in those conventions: International Covenant on Civil and Political Rights, 1966, Art 2(1); International Covenant on Economic, Social and Cultural Rights, 1966, Art. 2(2); International Convention on the Suppression and Punishment of the Crime of Apartheid, 1973; International Convention against Apartheid in Sports, 1985. Refer in this context also to Arts. 2 and 7 of the Universal Declaration of Human Rights, 1948, which, although it is not a legally binding treaty, is generally considered to be declaratory of binding customary international law. The following treaties prohibit racial discrimination in the specific fields with which they deal: Convention relating to the Status of Refugees, 1951, Art. 3; Convention relating to the Status of Stateless Persons, 1954, Art. 3; ILO Convention No. 111 concerning Discrimination in respect of Employment and Occupation, 1960, Art. 3(b); UNESCO Convention Against Discrimination in Education, 1962, Art. 3; Additional Protocol I to the Geneva Conventions on the Protection of Victims of International Armed Conflicts, 1977, Art. 85(4); Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment, 1984, Art. 1; Convention on the Rights of the Child, 1989, Art. 2.

group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof;

(b) Shall declare illegal and prohibit organizations, and also organized and all other propaganda activities, which promote and incite racial discrimination, and shall recognize participation in such organizations or activities as an offence punishable by law ..."

That States have a duty to enact legislation punishing the dissemination of racist propaganda and incitements to racial hatred has subsequently been reiterated in a number of declarations of international organisations and resolutions of international conferences, which may be considered as "international soft law". Art. 6 of UNESCO's 1978 Declaration on Race and Racial Prejudice[105] holds that "the State should take all appropriate steps, inter alia by legislation ... to prevent, prohibit and eradicate ... racist propaganda ..." Art. 7 of the same Declaration urges States to "adopt such legislation as is appropriate" to restrict "any propaganda, any form of organisation or any practice ... which seeks to justify or encourage racial hatred and discrimination in any form". The OSCE, at several of its intergovernmental meetings, declared the intention of the Member States to adopt such legislation as is necessary to provide protection against manifestations of racism and incitement to violence based on racial hatred[106]. Art. 1 of UNESCO's 1995 Declaration of Principles on Tolerance[107] states that tolerance, which necessarily involves respect for the social and cultural characteristics of other human beings regardless of their racial origins, is a "legal requirement" incumbent upon "individuals, groups and States". Finally, the General Assembly of the United Nations resolved in 1997 to express its deep concern at the misuse of the Internet by those who advocate racism, to "categorically deplore" the misuse of the Internet as a means of inciting others to violence motivated by racial hatred and to "[recognise] that Governments should implement and enforce appropriate and effective legislation to prevent acts of racism, racial discrimination, xenophobia and related intolerance"[108]. It is worth noting that none of these instruments expressly refer to revisionism.

4.2. Practice of States in respect of Article 4 of ICERD

At 1 January 2000, a total of 155 States were party to the ICERD. All Member States of the Council of Europe, except for Andorra, Liechtenstein, Moldova and San Marino, have either ratified, or acceded or succeeded to the ICERD. However, a total of 20

105 Adopted and proclaimed by the General Conference of the United Nations Educational, Scientific and Cultural Organisation at its 20th session, 27 November 1978. U.N. Doc. E/CN.4/Sub.2/1982/2/Add.1, annex V.

106 Refer to the: Document of the Copenhagen Meeting of the Conference on the Human Dimension, 29 June 1990, paras. 40 and 40.1; Document of the Moscow Meeting of the Conference on the Human Dimension, 3 October 1991, para. 38.1; CSCE Budapest Document – Toward a Genuine Partnership in a New Era, 6 December 1994, para. 25. A compilation of extracts from these documents is available at:

http://www.osce.org/odihr/them/discrim.htm.

107 Proclaimed and signed by the Member States in the General Conference of the United Nations Educational, Scientific and Cultural Organisation at its 28th session, 16 November 1995. This document is available at http://www.unesco.org/tolerance/declaeng.htm.

108 Points 11 and 12 of General Assembly Resolution No. 52/109, entitled "Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance", U.N. Doc. No. A/52/642, adopted without a vote on 12 December 1997. It is worthwhile to note that this resolution was prepared by the Third Committee, with responsibility for social, humanitarian and cultural matters, rather than the Sixth Committee, which has responsibility for legal matters.

States Parties to ICERD have entered reservations and/or interpretative declarations in respect of Art. 4, which have not been subsequently withdrawn[109].

Of the nine States which have subjected their acceptance of Art. 4 to reservations in the strict sense, only Switzerland is a Member of the Council of Europe. Three States (Japan, Nepal and Papua New Guinea) have subordinated their obligations under Art. 4 to the limitations of their own constitutions, while three other States (the Bahamas, Barbados and Jamaica) went so far as to rank their constitutions as superior to all of their obligations under the ICERD. The United States of America indicated its refusal to accept any obligation under Art. 4 which would require restriction of the protection afforded by its constitution and laws to the freedoms of speech, expression and association. Australia stated that it was not in a position to legislate for the introduction of the additional, specific criminal offences required by Art. 4, while Switzerland made an apparently inverse reservation of its "right to take the legislative measures necessary for the implementation of article 4, taking due account of freedom of opinion and freedom of association..."

Of the 15 States which lodged interpretative declarations in respect of Art. 4, six are Members of the Council of Europe (Austria, Belgium, France, Italy, Malta and the United Kingdom). Eight of the remainder are members of the Commonwealth and some of these States essentially adopted declarations which the United Kingdom had made on their behalf before they attained full independence. This substantial degree of homogeneity in the sources of declarations concerning Art. 4 is reflected to a large degree in their contents. Nine States (Austria, the Bahamas, Belgium, Fiji, France, Italy, Monaco, Tonga and the United Kingdom) indicated that they interpret the caveat that appears in the opening sentence of Art. 4, namely that measures should be taken "with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention", as meaning that States Parties retain the discretionary power to strike a proper balance between the freedoms of opinion, expression and peaceful association on the one hand, and the obligation to refrain from disseminating racist propaganda and inciting to racial hatred on the other hand. The Swiss communication quoted above, although it carries the title of a reservation, should be more correctly categorised as a declaration to the same effect. The eight Commonwealth States (Antigua & Barbuda, the Bahamas, Barbados, Fiji, Malta, Nepal, Papua New Guinea, Tonga and the United Kingdom) further indicated that they interpret paragraphs a) and b) of Art. 4 as requiring States Parties to enact additional or modified legislation only in cases where those States feel that such a step is necessary in order to achieve the objectives set out in the opening sentence of Art. 4.

No States Parties have lodged objections to any of these reservations or declarations concerning Art. 4. This is rather surprising, given that nine States lodged objections to the Saudi Arabian and/or Yemenite reservations of the right to apply the prescriptions of the Shari'ah, including a number of States (Denmark, Finland, Germany, Mexico, the Netherlands, Spain and Sweden) which had not entered reservations or declarations in respect of Art. 4 and most of which are incidentally

109 A list of ratifications and the texts of all reservations, declarations and objections lodged by States Parties to ICERD, maintained and regularly updated by the Treaty Section of the United Nations Bureau of Legal Affairs, may be found at:

http://untreaty.un.org/ENGLISH/bible/en...ternetbible/partI/chapterIV/treaty2.asp

Members of the Council of Europe. Given that Art. 20(2) of the ICERD invites States Parties to object to reservations which are incompatible with the objects and purposes of the Convention, but that this has not occurred in the 25 years since the Australian reservation and the six years since the United States' reservation was entered, it must be concluded that other States Parties consider these reservations to be permissible in the framework of ICERD. Similarly, the interpretations of Art. 4 suggested by the 15 States which lodged relevant declarations have been tacitly designated as acceptable by the remaining States Parties.

4.3. Opinions of specialised organs and jurists

The Committee on the Elimination of Racial Discrimination (CERD) created by the ICERD, in its General Recommendation XV (42) of 17 March 1993, stated its opinion that Art. 4 of ICERD is of a mandatory nature, obliging all States Parties to enact legislation which prohibits and punishes each of the acts mentioned in paragraphs a) and b) and to ensure that such laws are enforced by national courts and other organs of the State. Furthermore, it found that legislation prohibiting the dissemination of ideas based upon racial superiority or racial hatred is compatible with the human rights to freedom of opinion and expression and of peaceful assembly and association. This conclusion is justified by the principle that rights and freedoms may not be exercised in a manner which deprives others of the enjoyment of their rights and freedoms[110]. Legal restrictions which are necessary to ensure respect for the rights and reputations of other persons[111], to protect other persons from racial discrimination and racially motivated violence[112] and to advance public order and welfare in a democratic society are therefore permissible under international law[113]. Indeed, human rights generally may not be exercised in any manner contradicting the purposes and principles of the United Nations[114], which include the encouragement of "respect for human rights and for fundamental freedoms for all without distinction as to race ...[115]". In its above mentioned Resolution[116], the United Nations General Assembly formally took note of this Recommendation and affirmed "that acts of racist violence against others stemming from racism do not comprise expressions of opinion but rather offences". Similarly, the Human Rights Committee created under the International Covenant on Civil and Political Rights has held the legislative prohibition of racist speech to be a legitimate and proportionate restriction upon the right to freedom of speech[117].

The United Nations High Commissioner on Human Rights has convened a number of expert seminars[118] to consider the role of the Internet in the context of the fight

110 Universal Declaration of Human Rights, Art. 29(2).

111 International Covenant on Civil and Political Rights, Art. 19(3)(a).

112 International Covenant on Civil and Political Rights, Art. 20(2).

113 Universal Declaration of Human Rights, Art. 29(2).

114 Universal Declaration of Human Rights, Art. 29(3).

115 Charter of the United Nations, Art. 1(3).

116 General Assembly Resolution No. 52/109 (supra, n. 108), at point 4.

117 In the case of *JRT and the WG Party* v. *Canada*, Communication No. 104/1981, U.N. Doc. Supp. No. 40 (A/38/40), at p. 231 (1983).

118 The most recent was the Expert Seminar on Remedies Available to the Victims of Acts of Racism, Racial Discrimination, Xenophobia and Related Intolerance and on Good National Practices in this Field, held at Geneva on 16-18 February 2000.

against racism and racial discrimination. In discussions on point IV of the programme of the 1996 Seminar to Assess the Implementation of the ICERD with Particular Reference to Articles 4 and 6, participants generally agreed that paragraphs a) and b) of Art. 4 provide a sufficient legal basis for States Parties to legislate to prohibit organisations which disseminate racism over the Internet[119]. The recommendations of the seminar were however, limited to a general appeal to States Parties to adopt legislation in pursuance of their obligations under Art. 4 a) and b), with the representatives of Japan and the United Kingdom stating that their governments did not necessarily agree to or support these recommendations[120]. In discussions on point II.B. of the programme of the 1997 Seminar on the Role of the Internet in the Light of the Provisions of the ICERD, participants suggested that further study of the permissible restrictions on the right to freedom of expression would be necessary before any attempt is undertaken to prohibit racist propaganda on the Internet[121]. The seminar finally recommended that national criminal laws should be amended so as to punish racism on Internet and permit the prosecution of Internet service providers, but this recommendation was restricted in scope to those States which have already enacted laws criminalizing racial discrimination and the dissemination of racism[122].

Members of the CERD have repeatedly emphasised their opinion that States Parties are obliged by Art. 4 of ICERD to enact legislation which punishes the dissemination of ideas of racial superiority and hatred over the Internet, to the same degree as incitement to racial hatred and discrimination by means of printed documents, films or any other media[123]. They argue that Art. 4's reference to the duty of States Parties to have due regard to the rights and freedoms set out in Art. 5 and in the Universal Declaration, cannot be interpreted as absolving States Parties from the duty to enact legislation prohibiting and punishing the acts described in paragraphs a) and b) of Art. 4, because such an interpretation would deprive Art. 4 of mandatory force and incorrectly treat it as a text without legal effect[124]. The independent discretion left to States Parties by Art. 4 is limited, in the opinion of CERD, to deciding whether the prohibited acts should be punished by courts as criminal offences, or by administrative or regulatory bodies as less serious infringements of the law[125]. On the other hand, in his 1998 report to the Commission on Human Rights[126], the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression noted[127] with some degree of implied satisfaction, that the 1997 expert seminar discussed above was unable to obtain a consensus even on the formulation of a voluntary international code of conduct for Internet users and

---

Point 3 of the programme was dedicated to legal and technical questions about racism on Internet. We have not yet been able to obtain the documentation or conclusions of that seminar.

119 The official report of the seminar has been published as U.N. Doc. No. E/CN.4/1997/68/Add.1.

120 Refer ibid, para. 123.

121 Refer to para. 66 of the official report of the seminar, which has been published as U.N. Doc. No. E/CN.4/1998/77/Add.2.

122 Refer ibid, para. 158, headed "The role of existing national criminal law".

123 Report of the Seminar to Assess the Implementation of the ICERD with Particular Reference to Articles 4 and 6 (supra, n. 119), paras. 37 and 40; Report of the Seminar on the Role of the Internet in the Light of the Provisions of the ICERD (supra, n. 121), paras. 44 and 46.

124 Report of the Seminar to Assess the Implementation of the ICERD ... (supra, n. 119), para. 38; Report of the Seminar on the Role of the Internet ... (supra, n. 121), para. 43.

125 Report of the Seminar on the Role of the Internet ... (supra, n. 121), para. 43.

126 Presented to the 54th session of the Commission and published as U.N. Doc. No. E/CN.4/ 1998/40.

127 In para. 8 of point III.C. of his report.

service providers, because of concerns that such a document could be used to justify improper infringements of the right to freedom of expression. The Special Rapporteur characterised[128] the reservations and interpretative declarations entered by States Parties in respect of Art. 4 of ICERD as evidence that the necessary delicate balance between the right to be free from expressions of racial hatred and to be protected from incitement to racial discrimination and violence on the one hand, and the rights of freedom of opinion and freedom of expression on the other hand, has not yet been found at the level of public international law.

4.4. Conclusion

Public international law currently offers a framework, in the form of an international convention of potentially universal application, which could be used to effectively combat the dissemination of racism on Internet across the globe. While the great majority of States have already adhered to this framework, a not insubstantial number unfortunately take the view that the convention does not require them to enact enforceable national laws punishing the dissemination of racism or incitement to racial hatred. Amongst the States Parties which have expressly taken this stance are several countries of major practical importance for the Internet at the present time (Australia, Japan, the United Kingdom and the United States of America) and it appears that their reluctance to impose legislative constraints on racist speech extends to the Internet. Current prospects of attaining agreement on concrete measures to combat racism on Internet at the global level are therefore not good.

128 Ibid, para. 7.

V. SOFT LAW

5.1. Soft law instruments

5.1.1. Netiquette[129]

Because the Internet is such a new and unique medium, people are having difficulty establishing rules for its use. Out of sheer necessity, the users of the Net have, over the period of time since the network was born, tended toward certain rules of network conduct. This code of network ethics has been given many names over the years - the one that has seemed to stick, however, is "netiquette", a conjunction formed from "network etiquette".

The interesting and unique thing about netiquette in contrast to a hard-and-fast system of rules is that it allows room for interpretation. From the point of view of an Internet User[130], netiquette can be seen as a corollary of the Gentleman's Rule: "An Internet User, while using the Internet, shall conduct himself as a Gentleman and Responsible Citizen" There is nothing to stop someone from abusing the network. As with our daily actions with those around us, we must face the consequences of our behaviour. If years of network use have produced anything resembling a system of order, it is surely embodied in what is referred to as netiquette.

The netiquette rules as such are very vague and do not specifically mention racism.[131] The rules which are closest to our issue might be that nobody shall use a computer to harm other people and one shall use the computer in ways that show consideration and respect. Racial discrimination on the Internet would therefore violate netiquette.

---

129 Jougleux Philippe, « La criminalité dans le cyberespace », Thèse de droit des Médias, 1999, p. 127 et s.

Shea Virginia, Core Rules of Netiquette, Albion Books, San Francisco, 1994, http://www.albion.com/netiquette/book, a description of netiquette in English is lso available on the www site of the Netherlands ISPA http://www.nlip.nl/frames/frame2bi.htm : click on the item “netiquette”

130 http://jade.wabash.edu/wabnet/info/netiquet.htm Interpretation by WABnet, The Wabish College Digital Information System, Indiana.

131 http://www.fau.edu/netiquette/net/ten.html The Net: User Guidelines and Netiquette - by Arlene Rinaldi the ten commandments for computer ethics from the Computer Ethics Institute:

1.) Thou shalt not use a computer to harm other people.

2.) Thou shalt not interfere with other people's computer work.

3.) Thou shalt not snoop around in other people's files.

4.) Thou shalt not use a computer to steal.

5.) Thou shalt not use a computer to bear false witness.

6.) Thou shalt not use or copy software for which you have not paid.

7.) Thou shalt not use other people's computer resources without authorization.

8.) Thou shalt not appropriate other people's intellectual output.

9.) Thou shalt think about the social consequences of the program you write.

10.)Thou shalt use a computer in ways that show consideration and respect.

Netiquette covers not only rules for maintaining civility in discussions, but also special guidelines unique to the electronic nature of forum messages. For example, netiquette advises users to use simple formats because complex formatting may not appear correctly for all readers. In most cases, netiquette is enforced by fellow users who will vociferously object if one breaks a rule of netiquette.

Internet Providers are beginning to integrate netiquette into their contracts. For example, a large telecommunications company in Switzerland called Swisscom specifically referred to netiquette in its description of the "bluewindow" Internet Access Services:

> "C.1.4 The customer accepts the rules listed in the netiquette (inter alia spamming, mail bombs, transmission of unwanted e-mail advertising) and shall comply with them." (Bluewindow)[132]

The same provisions may be found in the general terms and conditions of the Austrian Provider Eunet.[133]

When netiquette is incorporated by reference in the general terms and conditions it becomes part of the contract and its violation constitutes a breach of contract. The fact that Internet Providers simply refer to netiquette without any further explanation or link to a detailed description implies that Internet Providers presume that what ought to be understood by the word "netiquette" is common knowledge – a presumption which may or may not prudent. Before incorporating the precepts of netiquette into a contract, Internet Providers should provide an explanation or at least a link to a description of the netiquette. We found an English description of the guidelines of the netiquette on the website of ISPA Netherlands.[134]

5.1.2. Codes of Conduct - Mechanism of self-regulation

For the industry to contribute effectively to restricting the flow of illegal and harmful content, it is also important to encourage enterprises to develop a self-regulatory framework through cooperation between them and the other parties concerned. This means that no access or hosting should be given by the Providers to illegal sites. The self-regulatory mechanism should provide a high level of protection and address questions of traceability. The Codes of Conduct are internal deals of the Providers who do not directly cooperate with the police. Some Internet Service Provider Associations have installed a hotline where illegal contents can be announced to the Providers and in this field they sometimes cooperate with the police. (see point 5.3. for examples)

---

132 See The blue window Internet Access Services - Service Description for "HighWay" http://www2.bluewindow.ch/info/index_e.html see point C.1.4

133 http://www.kpnqwest.at/services/agb.shtml see point 8.4. “Der Vertragspartner anerkennt die Notwendigkeit der Einhal-tung der "Netiquette". Sollten aus dem Internet Beschwerden über den Vertragspartner an KPNQwest herangetragen werden, so ist KPNQwest im Wiederholungsfalle berechtigt, den Anschluß und das Vertragsverhältnis mit sofortiger Wirkung aufzulösen. Weiters wird die zur Bearbeitung der Beschwerden benötigte Zeit mit dem zum jeweiligen Zeitpunkt von KPNQwest üblicherweise verrechneten Stundensatz dem Vertragspartner verrechnet."

134 http://www.nlip.nl/frames/frame2bi.htm http://www.nlip.nl/index.html Homepage of NLIP, click „beleid+informatie“, after „netiquette“, after „RFC 1855“.

5.1.3. General terms and conditions of Providers

In some countries the contracts between Providers and their clients - who buy space in or access to the Internet - are governed by general terms and conditions which incorporate Codes of Conduct. In the case of a breach of the Code of Conduct there is also a breach of the contract with the foreseen consequences (removal, closure, etc). Unified general terms and conditions for all Providers do not yet exist. There are different types of references concerning illegal contents on the net. Some of the General terms and conditions refer to illegal contents without any specification, others specify the prohibited acts such as racism, revisionism, or child pornography:

> "*User Guidelines for sunrise internet services (SUNRISE SWITZERLAND)*[135]
> Legal and illegal use:
> ... You are under obligation not to use the services provided for committing, or causing to be committed punishable offences and to take suitable measures to prevent illegal use by your employees or members of your household. This applies in particular to matters of illegal games of chance, money laundering, the publication and the making accessible the presentation of violence, so-called hard pornography, incitement to crime or acts of violence, disturbance of religious and cultural freedom or racial discrimination."

Some include a citation to the specific articles of the relevant laws.

> *The blue window Internet Access Services - Service Description for* "HighWay" (Switzerland)[136]
> C.1. Information content
> ...
> C.1.2. In particular, the following illegal information content may not be transmitted or made accessible via the customer's access:
> – Depiction of violence as defined in Art.135 of the Swiss Penal Code
> – Pornographic texts, photographs and depictions as defined in Art. 197 Clauses 1 and 3 of the Swiss Penal Code
> – Racial discrimination as defined in Art. 261bis 261bis of the Swiss Penal Code
> – Incitement to violence as defined in Art. 259 261bis of the Swiss Penal Code
> – Instruction or incitement to criminal offences or other encouragement of the same
> – Illegal games of chance (in particular in the scope of the Lottery Act)
> – Information which infringes copyright, related protection rights or intellectual property rights of third parties.

We found no Code of Conduct with more specific references. This is in fact a weak point of this type of self-regulatory mechanism. The more precisely defined the Codes of Conduct, as well as the general terms and conditions, the more aware users are of the fact that they are violating the law and that their acts are punishable.

---

135 http://www.sunrise.ch/en/gen_ter.htm see point 1.2, http://www.ispa.at/ click ISPA Verhaltensrichtlinien, http://www.kpnqwest.at/services/agb.shtml see point 8.11 allgemeine Geschäfts- und Lieferbedingungen der Eunet EDV-Dienstleistungs-Gesellschaft m.b.H.

136 http://www2.bluewindow.ch/info/index_e.html see C 1.2,
http://www.fsm.de/english/kodex/index.html see point 2.

In the interest of completeness, we must discuss the limits of Codes of Conduct in general terms and conditions. A very recent case concerns the Provider Yahoo. On 23 February 2000, Yahoo America was accused by the American Anti Defamation League of not respecting its own Charter of Codes of Conduct concerning illegal racist content on the net. Unlike Yahoo France, Yahoo America did not remove the site where one can buy Nazi objects which are sold by auction.[137] One reason for the American Provider Yahoo's reticence might be the more liberal approach to the freedom of speech in the U.S. (see infra).

5.1.4. Governmental Registration Boards and Hotlines

An effective way to restrict circulation of illegal material is to set up a network of centres (known as hotlines) which allow users to report content which they come across in the course of their use of the Internet and which they consider to be illegal.[138] There are several types of institutions to whom the illegal content may be announced, such as a governmental registration board or a hotline (often installed by Providers or ISPAs) or NGO's which also run hotlines. Responsibility for prosecuting and punishing those responsible for illegal content remains with the national law-enforcement authorities, while the hotlines aim at revealing the existence of illegal material with a view to restricting its circulation. Differences in national legal systems and cultures must also be respected. This means that in different countries different instruments are more easily accepted than others. We can say that sometimes the NGO is the first institution of contact concerning illegal contents. In other countries the Providers' hotlines are frequently used to announce illegal contents. Based on the experience with hotlines for contents concerning child pornography, we would like to stress the importance of not having too many different contact points for announcing illegal contents in order to allow for a comprehensive overview of the subject and to avoid having various institutions or entities working in parallel.

5.1.5. Instruments to trace illegal contents: filtering, rating, labelling[139]

To promote safer use of the Internet, it is important to make the content easier to identify. This can be done through a rating system which describes the content in accordance with a generally recognised scheme (for instance, where items such as sex or violence are rated on a scale) and by filtering systems which empower the user to select the content he/she wishes to receive. Ratings may be attached by the content provider or provided by a third-party rating service. There are a number of possible filtering and rating systems. However, their level of sophistication is still low and none has yet reached the "critical mass" where users can be sure that content in which they are interested and content which they wish to avoid will be rated appropriately and that perfectly innocuous content will not be blocked.[140]

---

137 http://www.zdnet.fr/actu/inte/a0013375.html „ Yahoo.com does not always comly with its anti-racist charter », ZDNet France, Internet Society, 11 March 2000.

138 http://www.fsm.de/bes/form/index.html "Beschwerdeformular" of the association "Freiwillige Selbstkontrolle Multimedia-Diensteanbieter" in Germany; http://hotline.ispa.at "Formular" of the Internet Service Providers Austria

139 For fuller information on the filtering systems and the adaption of the legislative framework of the information society, see the following sites : http://www.csa.fr/avecflash.htm and http://www.csa.fr/html/dos125.htm

140 An example of filtering by self-regulation concerning hypertext links:

http://www.droit.umontreal.ca/~farassef/cipertexte

The labelling[141] of a web site is a voluntary step by the publisher of the content or any other operator. It consists of labelling the content of the pages which the site contains and classifying them in various categories. This labelling/classification, which proceeds from the principle that information should be provided about the information, is designed to allow the end user of the computer to filter the contents to which he has access, whether he does this himself (i.e. by deciding not to consult the web pages whose labels do not appeal to him) or by means of purpose-designed software. Such is the nature of self-regulation that the labelling of web sites appears to have an essential role: piece: by this process the user tends to become responsible for the contents which he wishes to receive.

In the United States[142] two series of initiatives are worth mentioning because they are particularly well known.

1. The platform of the Recreational Software Advisory Council (RSAC), a non-profit-making association sponsored by the largest firms in the Internet market (IBM, Microsoft, Dell, Disney Online etc.) seeks, in particular, to divide websites into categories according to the types of public. At present the RSAC has classified approximately 50,000 sites, using as labelling criteria violence, sex, language and nudity.

2. SafeSurf is an organisation set up by Ray Soular and Wendy Simpson in 1995 to protect children on the Internet. A number of factors are taken into consideration for the purpose of labelling: profanity; heterosexual themes; homosexual themes; nudity; violence; sex, violence and profanity; intolerance, glorifying drug use; other adult themes; and gambling.

In Germany the *eco* (electronic commerce forum)[143] acts as a spokesperson and representative for the Internet industry. In 1996 they created a working group called *ICTF (Internet Content Task Force)* which specialised in scanning and rating of Newsgroups with illegal and harmful content, including racist content. The Providers can denounce Newsgroups which seem to contain illegal material.[144]

The described instruments should not only protect Internet users from being confronted with racist content on the net, but should also restrict the active research of racist material by search engines. As an example, let us return to Yahoo: Upon typing the Keyword "nazi" search engines of Yahoo, France will produce only scholarly works on nazism, as opposed to Yahoo, America's search engines, which continue to provide references to racist sites.

141 http://www.csa.fr/html/dos125.htm: see p. 18.

142 http://www.csa.fr/html/dos125.htm : voir p. 19

143 http://www.eco.de/408.htm

144 Information by Mr. Summa from eco (phone call 14 of march 2000)

5.2. European approach

5.2.1. Action Plan on the safer use of Internet[145]

The Action Plan shall cover a period of four years from 1 January 1999 to 31 December 2002. The financial framework for the implementation of the Action Plan for the period from 1 January 1999 to 31December 2002 has been set at ECU 25 million.

The action lines, in conjunction with the Recommendation on protection of minors and human dignity, are a means of implementing a European approach to safer use of the Internet, based on industry self-regulation, filtering, and rating and awareness. Strong support has been expressed for this approach at the level of the European Parliament and by the Council and Member States, as well as in the wider European context of the Bonn Declaration agreed to by Ministers from 29 European States.

5. 2.1.1. Creating a European network of hotlines

So far, hotlines exist only in a limited number of Member States. Their creation needs to be stimulated so that there are hotlines operating covering the Union both geographically and linguistically. Mechanisms for exchange of information between the national hotlines, and between the European network and hotlines in third countries need to be put in place.

In order for this network to develop its full potential, it is necessary to improve cooperation between industry and law-enforcement authorities, ensure Europe-wide coverage and cooperation, and increase effectiveness through exchange of information and experience.

This action will take the form of a call for proposals for participating organisations (20-25) to establish a European network of hotlines, and links between this network and hotlines in third countries, develop common approaches and stimulate transfer of know-how and best practice.

The participating organisations will be supported by a cross-section of industry actors (access and service providers, telecom operators, national hotline operators) and users. They will have to demonstrate a forward-looking and innovative approach, in particular in their relationship with national law-enforcement authorities.

5.2.1.2. Encouraging self-regulation and codes of conduct

In view of the transnational nature of communications networks, the effectiveness of self-regulation measures will be strengthened, at the European Union level, by coordination of national initiatives between the bodies responsible for their implementation.

145 Action Plan on Promoting Safer Use of the Internet, Decision No 276/1999/EC of the European Parliament and of the council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. http://www.echo.lu/home.html

Under this action line, it is foreseen to develop guidelines at the European level for codes of conduct, to build consensus for their application, and support their implementation. This action will be carried out through a call for tender to select organisations that can assist self-regulatory bodies to develop and implement codes of conduct. In connection with the establishment of Codes of Conduct, a system of visible "quality-Site Labels" for Internet Service Providers will be encouraged to assist users in identifying providers that adhere to Codes of Conduct. Measures will be taken to carefully monitor progress. This will be done in close coordination with the promotion of common guidelines for the implementation, at the national level, of a self-regulation framework as advocated by the Council Recommendation on Protection of Minors and Human Dignity.

5.2.1.3. Developing filtering and rating systems

Uptake of rating systems by European content providers and users remains low. The measures under this action line will focus on demonstrating the potential and the limitations of filtering and rating systems in a real world environment, with the objective of encouraging the establishment of European systems and familiarising users with their use. Filtering and rating systems must be internationally compatible and interoperable and developed with full cooperation of representatives of industry, consumers and users[146].

In this context we want to mention the INCORE[147] project (Internet Content Rating for Europe) funded as a Preparatory action to this EU-Action plan whose aim is to install a system which describes contents of websites. Founded by the European Commission (GD XIII) and hosted by Microsoft and UUnet its members are experts from the European Commission, representatives of private enterprises, private and public lobbying groups.

5.2.1.4. Encouraging awareness actions

Awareness is also the necessary complement of the described Action lines, since the actions of industry to implement self-regulation and filtering and rating will bear fruit only if users and potential users are aware of them.

The European Parliament has called for the implementation of a European campaign and an information and awareness action programme, to be funded by the EU budget, to inform parents and all people dealing with children (teachers, social workers, etc.) on the best way (including technical aspects) to protect minors against exposure to content that could be harmful to their development, so as to ensure their well-being.

European action, on the basis of actions undertaken by the Member States, will contribute to reinforcement of synergy, in particular through exchange of information and experience. The Action Plan will initiate awareness actions that will

146 http://www.csa.fr/avecflash.htm INCORE workinggroup

147 Description in comparison to other countries (esp. USA, France)

http://www.csa.fr/html/dos125.htm Adaptation of the legislative framework of the information society: the response of the CSA (Conseil Supérieur de l'audiovisuel) to the Government's guidelines, La Lettre du CSA n° 125 - February 2000, France.

build on the dissemination of information from access providers to customers, and also develop material for use in the education sector.

5.2.2. EuroISPA[148]

EuroISPA is the pan-European association of the Internet Services Providers associations of the countries of the European Union. The association was established when a number of such ISP associations signed the EuroISPA Memorandum of Understanding on 6 August 1997 in Brussels. On 10 September 1997 the signatories to the MOU met again and signed the agreement that formed EuroISPA EEIG, thereby creating the largest association of ISPs in the world.

From the aims and objectives:

> "EuroISPA is being established to achieve several important purposes. First, to protect and promote the interests of Europe as a whole within the global Internet, securing for Europe a premier position in the key industry of the new Millennium. Secondly, to help deliver the benefits of this new technology of liberation and empowerment to individuals, while at the same time meeting the legitimate concerns of parents and others responsible for the weaker members of society. Thirdly, to encourage the development of a free and open telecommunications market, something of great benefit to society as a whole but essential to the healthy development of the Internet. And finally, to promote the interests of our members and provide common services to them where these cannot be had elsewhere."

At this time the EuroISPA members are Austria, Belgium, Denmark, France, Germany, Ireland, Italy, the Netherlands, Spain, Finland and the United Kingdom.

5.3. Implementing soft law instruments by Internet Providers and NGOs

5.3.1. Austria

In Austria there is a Public Registration Board at The Ministry of Interior (*Polizeiliche Meldestelle im Innenministerium*) where anyone can report contents which he/she comes across in the course of their use of the Internet and which he/she considers to be illegal. This Registration Board is closely working together with the private hotline of the ISPA (*Internet Service Providers Austria)*[149]*.* This cooperation is functioning very well and is based on an informal agreement between the ISPA and the Registration Board who installed a so-called *Hotline Beirat* which consists of representatives of the public and private hotlines. The two institutions exchange Internet addresses with illegal and, especially, racial content in order to eliminate those websites.

Furthermore the ISPA has developed recommendations of Codes of Conduct[150] for its members. Since the big majority of Austria's Providers are members of the ISPA the acceptance of this self-regulation mechanism is very high. "To reach such a high

148 http://www.euroispa.org/

149 http://www.ispa.at/index.html

150 http://www.ispa.at/ click ISPA Verhaltensrichtlinien

level of application of self-regulation mechanisms it is necessary to follow an active information policy" says Karl Hitschmann, member of the direction of the ISPA.

The Austrian Internet-Provider EU-Net Austria[151] for example went one step further by implementing a paragraph concerning the netiquette and illegal contents in its general terms and conditions. EU-Net's clients are therefore bound to respect the legal norms punishing the dissemination of Nazi-propaganda otherwise the contract can be cancelled.

Another reason why all these mechanisms of self-regulation are working quite well is the fact that the Providers fear a certain responsibility for illegal contents. As long as there is no clear definition under the law of who is responsible for illegal contents on the net, the role of the Providers will remain an active one.

As non-governmental organisation we want to mention "helping hands"[152] which has also installed an antiracism hotline and is actively cooperating with the Discrimination hotline Internet in the Netherlands. (see supra)

5.3.2. The Netherlands[153]

In the Netherlands a self-regulatory mechanism has been installed between the police and the Providers. Probably comparable with the above described Austrian institution the "meldpunt discrimatie Internet" (Discrimination Hotline Internet, DHI) for discrimination deals with racial contents on the Internet where everyone can announce sites with illegal contents. There we could find a link to the Austrian NGO "helping hands".

DHI is a project of the Magenta foundation. The hotline is advised by the Anti Discrimination Bureau Amsterdam (MDA) and the National Attorney Discrimination Expertise Centre , supported by the Dutch branch organisation for Internet Providers (NLIP), the Ministry of Justice and the Ministry of Internal Affairs. The DHI was founded after an increase of racist and discriminatory statements on the Internet.

By sending a warning/request to remove the material, DHI tries to decrease the amount of racist and discriminatory statements on the Dutch part of the Internet. When material is not removed, DHI files an official complaint with the Dutch Police.

5.3.3. Germany

5.3.3.1. Code of conduct

The Association for Voluntary Self-Monitoring of Multimedia Service Providers[154] was established with the following aims. The preamble of its Code of Conduct dated from the 9 July 1997 provides:

---

151 http://www.kpnqwest.at/services/agb.shtml see point 8.4 and 8.11

152 http://www.helpinghands.at/Default.htm click English, click links: there you will find a link to the Magenta foundation in the Netherlands (see organisations against racism)

153 http://www.nlip.nl ISPA Netherlands

154 http://www.fsm.de/

"The Association for the Voluntary Self-Monitoring of Multimedia Service Providers ("Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V."; FSM in short) wishes to make its contribution toward strengthening the freedoms of Service Providers and protecting the valid interests of users and the general public, in particular against race discrimination and the glorification of violence, and to act on the basis of self-responsibility in order to strengthen protection for youth. Any form of censure will be rejected.
The Association for the Voluntary Self-Monitoring of Multimedia Service Providers wants to encourage Service providers to join in order to make them abide by the principles of the Code of Conduct and punish any violations of this code."

Up to now, approximately 300 German enterprises agreed to accept the Code of conduct of the FSM. Almost every day new supporters join the association. In the first year of its existence the FSM had to deal with 200 complaints. One can therefore say that the FSM is the most widely accepted Online-Self regulation institution in Germany.[155]

Principles of conduct - Impermissible content [156]
"The members of the Association for the Voluntary Self-Monitoring of Multimedia Service Providers shall take all actions, within the scope of legally determined responsibility and to the extent actually and legally possible and reasonable, to ensure that content which is unlawful or impermissible, in particular pursuant to
a) § 130 of the StGB (Incitement to hatred and violence against segments of the population (or minority groups) or publishing insults against them in such a manner as to endanger the peace or to expose them to scorn or contempt);
b) § 130a of the StGB (Incitement to commit crimes);
c) § 131 of the StGB (Depiction of acts of violence, instigation to racial hatred);
... is neither provided nor switched for use."

5.3.3.2. Tasks and intentions of the FSM-Beschwerdestelle (Complaints Office)

Anyone is entitled to complain to the Complaints Office of the Association "Voluntary Self-Control for Multimedia Service Providers" with respect to contents which are available on the Internet or on any other networks or via online services. Complaints which are received by a member may be forwarded to the Association.

The commissioner at the Complaints Office (Commissioner) shall be responsible for the initial review of complaints received. In addition, complaints shall be treated by the Complaints Office and by its Chairperson in accordance with §§ 5 et seq of the *Beschwerdeordnung* where a decision-making procedure is laid down and on the basis of the Code of Conduct instituted by the Association.

155 http://www.fsm.de/ueb/index.html

156 http://www.fsm.de/english/kodex/index.html

The *FSM-Beschwerdestelle* is not competent concerning complaints which are contents of individual communication systems, for example insults or pornographic contents which are communicated by e-mail. It is also not competent concerning contents of Newsgroups. Under the conditions of § 6a of the *Beschwerdeordnung* the head of the *FSM-Beschwerdestelle* can inform the competent state institutions.

A collaboration with the Police authorities or the public Prosecutor's Office is in principle excluded. In exceptional cases, if there is a strong suspicion of danger for life and health of the persons shown on the net, especially in cases of child pornography, the competent authorities are informed.

5.3.4. France

5.3.4.1. General

L'AFA (l'Association des Fournisseurs d'Accès et de Services Internet) réunit en son The AFA (Association of Access and Internet Service Providers) is made up of the following providers of Internet access and/or services: AOL Bertelsmann France, Cegetel, CompuServe France, FranceNet[157], France Pratique, France Telecom Interactive, Grolier Interactive, Imaginet, Infonie, Internet Way, 9 Telecom, Business-Village, chello France, Club-Internet, France Explorer, Freesbee, Isdnet, Lokace, Lyonnais Cable, Magic Online, Uunet France, Wanadoo, World online France and Yahoo! France. The *Practices and Uses* of January 1998[158] contain a first code drawn up by its members. There is no express reference to racist sites, but only to the concept of netiquette (see point I.1 of the *Practices and Uses*).

The AFA has also opened a *Point de contact* (contact point) to help react to what are presumed to be illegal contents on the Internet. *AFA Point de Contact* provides information on the criminal provisions applicable to paedophilia and incitement to racial hatred and helps users to understand what they can do when they find illegal contents of that type via the Internet.

Since November 1999 a preliminary inquiry into the establishment of a joint Internet regulatory body has been in progress within the Government Information Service of the Prime Minister of France. Joint regulation represents a combination of market regulation, regulation by the community of users and regulation by law. The joint regulatory body must act with complete independence, but there is no question of establishing an independent administrative authority with competence for the Internet. The main areas for such a body are above all the ethics of the contents, consumer protection and the code of conduct of the actors. The body could be a forum for reflection and information, it could encourage self-regulation and participate in combating illicit contents[159].

157 http://www.francenet.fr

158 http://www.afa-france.com/html/action/index_usages.htm

159 Preliminary inquiry into the establishment of a joint Internet regulatory body, under the presidency of Christian Paul, Deputy for la Nièvre, November 1999/March 2000, http://www.internet.gouv.fr/francais/index.html: click on "recherche" and type in the keyword "corégulation".

5.3.4.2. Is netiquette legally binding

Reference has already been made to netiquette in the context of a dispute before the courts. In the *Estelle Hallyday* case the court of first instance considered that "the host is under an obligation to ensure that those he accommodates observe proper moral standards, that they comply with the ethical rules governing the web ..."[160]. Netiquette was therefore referred to, but it was used in a strange way: compliance is not a matter for the user, who is none the less the theoretical addressee of this primarily moral text, but for the professional responsible for the user. If netiquette continues to be extended in this way, it will be necessary to debate the precise content of netiquette, which at present is particularly vague. Although its use in a civil context is not necessarily a cause for alarm, it might seem more unusual if the provisions of netiquette should be used as an argument in criminal proceedings[161].

Several types of contract may well take netiquette into account for the purpose of inserting it into the list of obligations of one or both parties. Netiquette then becomes legally binding, in the same way as an annex setting out general conditions or a reference in the contract to a special clause.

However, the contracts which refer to netiquette are frequently standard-form contracts. That is the case, in particular, of contracts for the provision of Internet access, which are certainly standard-form contracts (it is frequently possible to peruse the contract only after a subscription has been taken out) and which sometimes contain a clause on netiquette, either express or, more commonly, implied. Thus in the general conditions of "Wanadoo", the access provider service of France Telecom, it is stated that the user must take note of the fact "that the community of Internet users has developed a code of conduct and that any person in breach of that code may be excluded from access to the Internet ..."[162]. Or again, the Internet access provider does not accept responsibility until the user has taken a positive step to "be familiar with the codes of conduct, uses and rules of behaviour which from time to time are disseminated on the Internet for that purpose"[163].

> Canadian case-law provides a very interesting example of a case where the court took netiquette directly into consideration; the case was *Ontario Inc.* v *Nexx Online Inc.* (Supreme Court of Ontario, Case 1267632/1999). It was summarised as follows by Lionel Thoumyre in the electronic review Juriscom.Net[164].
>
> This is the first Canadian decision in a case concerning unsolicited mail ("junk mail" or "spam") and the implementation of the rules of netiquette.

160 Paris Regional Court, 9 June 1998 *Estelle* v *Valentin and Daniel*, at website legalis.net

161 Jougleux Philippe, *La criminalité dans le cyberspace, Thèse de droit des Médias*, 1999, p. 132.

162 General conditions available at the following address:
http://www.wanadoo.fr/wanadoo-et-moi/offre/html/conditions_occ/html
See Article 6.

163 General conditions of "Club-Internet", the Internet service of Grolier Interactive, at: http://www.cybertheque.fr/conditions.html See point 3.1.5

164 Interview on self-regulation with Professor Pierre Trudel, in the "Professionels" space on Juriscom.net, case summarised by Lionel Thoumyre; http://www.juriscom.net/jurisca/spamca.htm

An Internet service provider in Toronto, Nexx Online, decided to close the accommodation account of its customer, company 1267632 Ontario Inc., which operated the site Beaverhome.com. The following reasons were given: since 31 March 1999 Beaverhome.com had sent more then 200,000 unsolicited messages each day through the services of another service provider. This practice is deemed to be contrary to the rules of the well-known netiquette to which the accommodation contract expressly referred. The customer none the loss considered that Nexx Online was not justified in disconnecting its site and decided to sue for breach of contract.

On examining the terms of the accommodation contract, Judge Janet Wilson pointed out at the outset that there was no obvious clause prohibiting Nexx Online's customer from distributing unsolicited commercial messages. However, she cited two contractual clauses in favour of the defendant:

1. the customer agrees to observe netiquette. This clause is drafted as follows: "Account Holder agrees to follow generally accepted 'netiquette' when sending e-mail messages or posting newsgroup messages ...";

2. a second clause provides that the customer may have to agree to new contractual provisions being added by Nexx Online (with the option of a refund should he refuse).

The president of Nexx Online informed the customer in August 1998 that unsolicited commercial e-mail could not be distributed through his services.

The significance of the judgment lies essentially in Judge Wilson's argument, which has the effect of conferring legal force on the rules of netiquette by means of the contract[165]. The judge then concludes that sending unsolicited advertising e-mail is clearly in breach of the emerging principles of netiquette, unless the service provider has expressly allowed it.

Finally, Judge Janet Wilson has no hesitation in finding that the defendant acted in breach of the terms of the contract, in so far as the contract refers the customer to the requirement to comply with the principles of netiquette. Thus the practice of spamming, contrary to the code of ethics in force on the Network, justified disconnecting the Beaverhome.com site: "31 (...) I conclude that sending unsolicited bulk commercial e-mail is in breach of the emerging principles of Netiquette, unless it is specifically permitted in the governing contract. As the rules of Netiquette govern the parties' Contract, the plaintiff is in breach of its terms justifying disconnection of service. Secondly, in the alternative, Nexx is permitted to add terms to the Contract precluding a Nexx client sending unsolicited bulk e-mail directly, or through a third party. If the plaintiffs do not concur with the new term, they are entitled to a rebate of the pro-rated balance of the Contract price, and the defendant is entitled to disconnect service.

165 First, the court inferred the unwritten netiquette rules on spamming from a series of documents: an author by an American author (John Levine, "Why is spam bad?": http://spam.abuse.net/spambad/html) and four United States judgments (*Cyber Promotion Inc.* v *American Online Inc.* E.D Pa. Nov. 4 1996: *CompuServe Inc.* v *Cyber Promotions Inc.* S.D. Oh. Feb 3 1997; *Parker* v *C.N. Enterprises* Tex. Travis County Dist. Ct. Nov. 10 1997; *Cyber Promotions Inc.* v *Apex Global Information Services Inc.* E.D. Pa. Sept. 30 1997).

The defendant has agreed to repay the prorated balance owing under the Contract from April 5, 1999 to August 5, 1999."

It should be observed that in Quebec netiquette may be binding on contracting parties, even in the absence of clauses expressly referring thereto, on the basis of Article 1434 of the Civil Code: "A validly made contract is binding on those who concluded it not only in respect of what they have expressed but also in respect of what follows from it according to its nature and in accordance with custom, equity or the law".

5.3.5. Belgium

The Code of Conduct of the ISPA in Belgium[166] includes an obligation to observe the law in general and to stet up a contact point where illegal contents may be reported.

"The police shall set up a Contact Point[167] to receive any complaints relating to any illegal or immoral activity (sexual activity, pornography, paedophilia – although this list is not exhaustive), racism and xenophobia, the negation of genocide, the provocation or encouragement of criminal acts, criminal association, games and lotteries, drugs or similar substances (for example sites offering for sale substances prohibited in Belgium) ... this list is not exhaustive."

5.3.6. United Kingdom

5.3.6.1. Code of Practice for ISPs

By virtue of the ISPA's very wide coverage of the Internet industry at retail level the most important item of soft law in the United Kingdom is its Code of Practice, last updated on 15.01.1999.[168] This code is contractually binding upon all ISPA members. It mentions racism on Internet in point 2, headed "General Requirements". According to point 2.2, sub headed "Decency", member ISPs are obliged to use best endeavours to ensure that their services and promotional material do not contain material which incites racial hatred or otherwise promotes or facilitates practices which contravene British law. However, this obligation is expressly formulated so as to exclude "Third Party Content". We have received confirmation that the ISPA does not make ISPs in any way responsible for material created by others, which they are hosting on their servers. If anyone, including the ISPs themselves, are unhappy with the contents of any websites or Usenet postings hosted, they should pass the relevant information to the IWF (Internet Watch Foundation[169]) to be dealt with.[170] The most

166 http://www.ispa.be/fr/c040201.html see point 3.3 of the Code of Conduct.

167 http://www.ispa/be.fr/c040202.html Protocol on collaboration to combat illicit acts on the Internet: "... 2. An Internet user may report any content which is presumed to be illicit via e-mail (contact@gpj.be) directly to the central judicial contact point, or contact his ISP".

168 http://www.ispa.org.uk/practise.html

169 The Internet Watch Foundation (IWF) http://www.iwf.org.uk/about/about.html was launched in late September 1996 by PIPEX founder Peter Dawe to address the problem of illegal material on the Internet, with particular reference to child pornography. It is an independent organisation to implement the proposals jointly agreed by the government, the police, the two major UK service provider trade associations, ISPA and LINX, and Mr Dawe. Science and Technology Minister Ian Taylor welcomed the proposals as "a major industry-led initiative to reassure the public and business that the Internet can be a safe and secure place to work, learn and play."

important element of the Code of Practice, for the purposes of combating illegal material on Internet, is therefore point 5, headed "IWF", which obliges member ISPs to comply with "take-down notices" issued by the IWF.

The IWF intends to play a more active role specifically concerning racism on the Internet. Under plans announced by the IWF Chairman and its Assistant Chief Executive and supported by the British Minister for Small Business and E-Commerce, Internet sites in the United Kingdom which publish criminally racist material are to be targeted for the first time by the IWF[171].

5.3.6.2. Technical Aspects of identifying authors of racist material

In May 1999, LINX (London Internet Exchange) published a document setting out the "Best Current Practice on Traceability".[172] It reflects neither the legal requirements nor the existing practice of the majority of British ISPs. Instead, it sets out goals for ISPs to reach for, so as to improve their ability to trace the source of any material inappropriately placed on Internet (illegal material, spam, falsely labelled material), to identify hackers or fraudsters operating over the Internet. That is also important for racist sites in order to find out who put the content on the net.

5.3.7. Italy

An association of providers and other communications operators, the ANFoV (*Associazione per la convergenza nei servizi di comunicazione*) has adopted a code of self-discipline[173], which has been in force since 1 January 1998. This code lays down procedures for reporting illicit contents, sets up a Self-disciplinary committee and provides for the application of penalties (in particular Articles 13 and 15 to 17). Thus far no racist sites have been reported. The code is not generally applicable, however, but must be accepted by the providers belonging to the association.

A draft self-regulation code intended to have a wider scope was prepared in 1997 by a working group consisting of the Associazione Italiana Internet Providers (AIIP), the Italian member of EuroISPA, and other organisations and associations of providers. The first draft is published on the AIIP's home page[174]. It has been the subject of lengthy discussion and a number of amendments have been made: a more recent version, dated 5 March 1998, has been published by the electronic review Interlex[175]. However, the participants in the working group have been unable to agree on a definitive text, which explains why the ANFoV decided to adopt its own code (see above) and why the text is still at the draft stage.

According to this draft, access providers and contents providers undertake to remove from their servers any manifestly illicit or offensive content (cf. Article 11). The code provides for the establishment of a "self-regulatory board" empowered to take

170 Mr. Nicholas Lansman, ISPA representative.

171 "Watchdog moves to curb racist websites", The Guardian, 30 January 2000.

172 It is available online at http://www.linx.net/noncore/bcp/illegal-material-bcp.html

173 http://www.anfov.it/codice.html

174 http://www.aiip.it/autoreg.html

175 http://www.interlex.com/regole/carta23htm

decisions on the implementation of the code and also to impose penalties (Articles 18 to 20). An appeal against the board's decisions will lie to a committee responsible for implementing the code (Article 21).

According to the information received from the AIIP, the principles forming the basis of the code are observed by the members of the association. However, the control procedure has not been implemented.

5.4. Implementing soft law instruments by governmental bodies

5.4.1. Switzerland

In September 1995 a working group formed within the Federal Office of Justice and consisting of senior officials (from, *inter alia*, the criminal law division, the Federal Institute for Intellectual Property, the Federal Officer for Data Protection and the Federal Office for Information Technology), undertook to investigate the most appropriate ways of combating abuse on the Internet. The experts' report, which was delivered six months later, was categorical on at least one point: the Swiss legislative machinery should not be reinforced but self-discipline should be encouraged among the operators, in particular access providers, by means of official recommendations[176].

This working group deserves recognition for not having merely formulated a general strategy but for having made eleven specific recommendations to access providers. These are essentially based on two types of measure: the blocking of illicit data and contractual restrictions. Thus:

(a) an access provider which has clear evidence that illicit data are being conveyed on its network must take the necessary measures to block consultation of such data; this applies not only to violent, pornographic or racist contents but also to contents which infringe copyright or similar rights;

(b) the access provider must reserve the right under the terms of the contract to cancel the subscription contract of any customer who disseminates illicit contents or allows such contents to be consulted through his connection; similarly, the contract will state that customers are required to observe copyright and similar rights.

For example, passages containing these recommendations have been included in the general conditions of the provider Sunrise[177]. Sunrise is very active in the area of self-regulation and has set up an e-mail address where cases of breach of the regulations can be reported. In addition, Sunrise has specialists who look for sites which do not comply with their general conditions. Where possible, they block sites with illegal contents.

176 *Le Nouveau média interroge le droit*, Report by an inter-departmental group on questions criminal law, data-protection law and copyright raised by the Internet (http://www.admin.ch/bj/infrecht/internet/inbearbf.htm).

177 http://ww.sunrise.ch/gen_ter.htm see 1.2, 6.3 and 6.9

Finally, there is the initiative known as "Aktion Kinder des Holocaust" in Basel[178], which requests Internet providers to block racist sites. Although Sunrise, Datacom and Swisscom-section IP Plus comply with such requests, Swissonline and CompuServe do not do so and do not block Internet sites without a court order.

5.4.2. Sweden

On 22 December 1999 the Commission for Information Technology (*IT-kommisionen*) submitted a proposal to the Government for the establishment of an ombudsman for ethics on the Internet, on the model of the ombudsmen already in office in Sweden (cf., for example, the ombudsman for the press or the ombudsman against discrimination). The idea is to promote dialogue with the various actors on the Internet in order to combat illicit contents effectively. At the same time, the Commission states that it is not in favour of drawing up codes of conduct or making recommendations in that regard. The ombudsman, who would be chosen from among persons of integrity enjoying the respect of the actors on the Internet, should be supported in his work by an ad hoc committee which would determine questions of principle. The ombudsman would have no power to take decisions.

The Government have not yet reached a decision on that proposal[179].

178 http://www.akdh.ch

179 The proposal can be accessed at http://www.itkommissionen.se/skrivels/sk991222.html

VI. CONCLUSION

At the close of this study, we find that:

- the European countries which we have examined have adequate legal instruments to combat racism: since they make no reference to a technical means of communication, the existing rules intended to combat traditional hateful statements are perfectly capable of suppressing hateful statements on the Internet. If there is any deficiency, it is solely in relation to the suppression of revisionism, since some European countries refuse to make the negation of genocide an offence.

- the difficulties encountered in combating racism on the Internet are due to the particular characteristics of communication on the Internet and to legal obstacles to the implementation of the practical rules prohibiting hateful statements.

  - for this reason, racist messages and the www sites which accommodate them are difficult to locate and their authors are difficult, since the information may be conveyed in an encrypted and anonymous form on the Internet; similarly, it may disappear very quickly from one server and reappear on another (a mirror site) on the other side of the world; finally, access providers do not keep records of the connections by surfers (logs) for a period long enough to enable the offending information to be traced back to its source.

  - the very wide protection which American courts afford to freedom of expression has allowed numerous racist www sites or electronic mailboxes to find refuge in the United States; where conduct in question does not constitute an offence in that country, judicial cooperation is inoperative: the authors of these racist communications cannot be prosecuted and the hosts cannot be compelled to close down the offending sites. This applies even more to revisionist statements: not only the United States but the more permissive European countries are so many "havens" for revisionism.

  - the legal instruments at the source of international judicial cooperation have not adapted to the era of digitalised, world-wide electronic communications. Their lengthy and cumbersome procedures, which are linked with national sovereignty, scarcely favour the cooperation and coordination indispensable to effective action against transient communications which know no frontiers.

- these difficulties in implementing judicial proceedings against the authors of racist statements have resulted in action being targeted against the various intermediaries who enable messages to be conveyed on the Internet: access providers and hosts in particular. In legal terms, the solutions found by the courts, and more rarely by the legislatures of the countries studied, are not yet uniform, but a certain tendency is emerging towards establishing a graduated scale of criminal, or even civil, liability, according to the proximity of the operator to the

content of the messages: an obligation to exercise diligence is imposed in the hosts and a fortiori on the relayers of information who operate electronic mailboxes or archives. On the other hand, access providers, who are more remote from the content, are prosecuted only if a judicial authority has informed them of the illicit nature of the information which they convey and has formally ordered them to block access to it.

- A movement to mobilise the community of surfers in order to locate racist and more generally illicit sites and to curb their proliferation is under way; the methods implemented vary between labelling sites and setting up hot lines; they also include filtering. Owing to the pressure brought to bear on them, the technical intermediaries, especially the access providers and hosts, have taken or are in the process of taking self-disciplinary measures in the form of codes of conduct, which are passed on to their customers by means of clauses inserted in the contracts prohibiting them from making unlawful use of the services provided.

On the basis of the foregoing, we are of the opinion that the following measures might be envisaged:

- At international level, a specific international convention aimed at suppressing racism on the Internet will have practical effect only if all the States in the world are parties to it. That is a utopian vision, in view of the considerable disparities regarding freedom of expression. The prudent course, therefore, would be to enter into a dialogue with all service providers, in particular the Americans, in order to convince them that they themselves must take the appropriate measures to combat racist sites (by blocking sites, filtering, refusing anonymity to authors of sites, etc.).

- On a material level, revisionism should be made an offence throughout Europe; although such standardisation on a continental scale will not prevent revisionist sites from finding a refuge in more permissive countries, it would send out a clear signal of the European attitude to revisionism.

- Again on a material level, it will be necessary to distinguish the function of the access provider from that of the host and to establish clearly the responsibility of each of them. Whereas the access provider should only be held responsible in respect of the illicit contents of which he was aware but to which he has not blocked access, the host must show that he has exercised wider vigilance, in particular towards sites which he accommodates anonymously and free of charge.

- In terms of procedure :

➢ it is important to ensure that national and international provisional measures make it possible to order manifestly racist sites or electronic mailboxes to be closed down as quickly as possible, or to block access to them.

- access providers must be required to keep logs of connections for six months; however, a longer period might be incompatible with the data-protection principle that information must not be stored indefinitely.

- hosts must be required to reveal the identity of the authors of the sites which they accommodate.

- on an ethical level, the efforts to achieve self-discipline made by access providers and hosts should be encouraged. The emphasis must be placed on making self-discipline more widespread: all access providers and hosts must comply with the ethical rules; in that regard, it is advantageous if there is a national federation to which all technical intermediaries belong.

- in a dynamic and changing environment, the dialogue between surfers, technical operators and prosecuting authorities must be preferred to misplaced and selective reactions on the part of the legislature. Setting up a body for dialogue, or indeed a joint regulatory body, is the most appropriate means of doing this; this body could participate in the preparation of codes of conduct, serve as mediator in specific disputes and act as a permanent observatory, in particular by informing the legislature of the measures to be taken when self-discipline does not work.

- education and training must be maintained. Education primarily concerns the community of surfers, especially children, who must be aware that they may encounter racist sites and that the statements which they will find are unacceptable. Training is especially aimed at the prosecuting authorities, who must know more about the specific technical features of the Internet; from this aspect the establishment at national level of a specialised prosecution authority would be an advantage.

- lastly, it must be emphasised that these various measures, in particular the obligation to exercise diligence, must not be aimed solely at combating racism, but also at combating any illicit communication on the Internet. In that regard, it would be appropriate to act in cooperation with those who seek to combat paedophilia on the Internet, since their action is particularly specific.