Strasbourg, 29 November 2002 CDMM (2002) Misc 18

DRAFT DECLARATION ON FREEDOM OF COMMUNICATION ON THE INTERNET

The member States of the Council of Europe,

Recalling the commitment of member States to the fundamental right to freedom of expression and information, as guaranteed by Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms;

Considering that freedom of expression and the free circulation of information on the Internet needs to be reaffirmed;

Aware at the same time of the need to balance freedom of expression and information with other legitimate rights and interests;

Recalling in this respect the Convention on Cybercrime and Recommendation No. R (2001) 8 on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services);

Recalling furthermore Resolution No. 1 of the 5th European Ministerial Conference on Mass Media Policy (Thessaloniki, 11-12 December 1997);

Concerned about attempts to limit access by the public to communication on the Internet for political reasons or other motives contrary to democratic principles;

Convinced that there is a necessity to state firmly that prior control of communications on the Internet, regardless of frontiers, should remain an exception;

Considering furthermore that there is a need to remove barriers to individual access to the Internet, and thus to complement measures already undertaken to set up public access points in line with Recommendation No. R (99) 14 on universal community service concerning new communication and information services;

Convinced that freedom to establish services provided through the Internet will contribute to guaranteeing the right of users to access pluralistic content from a variety of domestic and foreign sources;

Convinced also that it is necessary to limit the liability of intermediaries when they act as mere transmitters or when they provide in good faith access to or host content from third parties;

Recalling in this respect Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market;

Stressing that freedom of communication on the Internet should not prejudice human dignity, human rights and fundamental freedoms of others, especially minors;

Considering that a balance has to be found between respecting the will of users of the Internet not to disclose their identity and the need for law enforcement authorities to trace the authors of criminal deeds;

Welcoming efforts by intermediaries to co-operate with law enforcement agencies when faced with illegal content on the Internet;

Noting the importance of co-operation between these agencies in the fight against such content;

Declare that in the field of communication on the Internet, they seek to abide by the following principles:

Principle 1 – Content rules for the Internet

Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery.

Principle 2 – Self-regulation or co-regulation

Member States should encourage self-regulation or co-regulation regarding content disseminated on the Internet.

Principle 3 – Absence of prior state control

Public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communications on the Internet, regardless of frontiers. This does not prevent the installation of filters for the protection of minors, in particular in places accessible to minors such as schools or libraries.

Provided that the safeguards of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms are respected, measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality.

Principle 4 – Removal of barriers to the participation of individuals in the information society

Member States should foster and encourage access for all to Internet communications and information services on a non-discriminatory basis at an affordable price. Furthermore, an active participation of the public, for example by setting up and running individual web sites, should not be subject to any licensing or other requirements having a similar effect.

Principle 5 – Freedom to provide services via the Internet

The provision of services via the Internet should not be made subject to specific authorisation schemes on the sole grounds of the means of transmission used.

Member States should seek measures to promote a pluralistic offer of services via the Internet which caters to the different needs of users and social groups. Service providers should be allowed to operate in a regulatory framework which guarantees them non-discriminatory access to national and international telecommunication networks.

Principle 6 – Limited liability of intermediaries for Internet content

Member States should not impose on service providers a general obligation to monitor the content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity.

Member States should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet.

In cases where the functions of service providers are wider and they store content emanating from other parties, members States may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.

When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information.

In all cases, the above-mentioned limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law.

Principle 7 – Anonymity

In order to ensure protection against on-line surveillance and to enhance the free expression of information and ideas, member States should respect the will of users of the Internet not to disclose their identity. This does not prevent member States from taking measures and co-operating in order to trace those responsible for criminal deeds, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.

DRAFT EXPLANATORY NOTE

1. Introduction

New communications and information technologies, commonly referred to as the "Internet", have opened up new horizons of public access to information, education and cultural resources. At the same time, the Internet provides an amazing tool for individual and group expression with possibilities of reaching a much larger audience than before at a low cost.

In recent years, the Council of Europe has adopted several legal and political instruments, which provide answers to the regulatory challenges posed by the Internet. The Convention on Cybercrime, opened for signature in 2001, enables mutual assistance between States regarding certain computer-related crimes. Another example is Recommendation Rec (2001) 8 on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), which deals with the issue of illegal and harmful Internet content in general, advocating a self-regulatory approach, with a view to protecting freedom of expression and information as well as other fundamental values.

Over the past few years, there has been a marked tendency by some governments to restrict and control access to the Internet in a manner which is incompatible with international norms on freedom of expression and information. Against this background, the Steering Committee on the Mass Media (CDMM) of the Council of Europe decided to draw up a Declaration where such practices, especially when politically motivated, would be strongly condemned. It was considered appropriate to deal in the same text with other aspects of the Internet where freedom of expression and information is particularly at stake, namely regarding the removal of barriers to the participation of individuals in the information society, the freedom to provide services via the Internet, the liability of intermediaries, as well as anonymity.

A first draft of this Declaration was made available for public comment on the web site of the Council of Europe in April 2002. Several organisations and individuals sent in their comments and they have been duly taken into account during the finalisation of the draft.

2. Commentary on the principles of the draft Declaration

Principle 1 - Content rules for the Internet

This principle stresses that member States should not apply prohibitions to Internet content which go further than those applied to other more traditional media; content which is legal off-line should also be legal on-line.

This principle was advocated in a joint statement of the UN Special Rapporteur on freedom of opinion and expression, the OSCE Representative on freedom of the media and the OAS Special Rapporteur on freedom of expression, dated 22 November 2001.

Principle 2 – Self-regulation or co-regulation

As already underlined in Recommendation Rec (2001) 8, member States should favour self-regulation or co-regulation regarding content disseminated on the Internet rather than regulation by the State. The need for setting up specific Internet regulatory bodies has not

been demonstrated. However, it could happen that some member States decide to set up such bodies, or entrust an existing regulatory body with the legal competence to regulate Internet content. In this event, such bodies would have to meet the requirements of Recommendation Rec (2000) 23 on the independence and functions of regulatory authorities for the broadcasting sector, in particular with regard to their independence from political and economic powers and the possibility to subject their decisions to judicial review.

Since such regulatory bodies would deal with issues affecting freedom of expression and information, it is necessary to recall that they should also respect Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

Principle 3 – Absence of prior state control

This principle underlines the importance of no prior state control over what the public can search for on the Internet. In some countries, there is a tendency to block access by the population to content on certain foreign or domestic web sites for political reasons. This and similar practices of prior State control should be strongly condemned.

Although the State should by no means take broad measures to block undesirable content, exceptions must be allowed for the protection of minors. Where minors have access to the Internet, for example in schools or libraries, public authorities may require filters to be installed on computers to block access to harmful content.

The absence of prior control by the State does not of course rule out measures being undertaken to remove content from the Internet or block access to it following a preliminary or final decision of the competent national authorities on its illegality, not only under penal law, but also under other branches of law such as civil or administrative law. This would typically be the case when injunctions are sought to prevent the publication on the Internet of content which is illegal. Such measures, which could entail some sort of prior control, would have to fulfil the requirements of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms and they would have to be directed at a clearly identifiable Internet content.

Principle 4 - Removal of barriers to the participation of individuals in the information society

This part of the Declaration builds on principles already established in Recommendation No. R (99) 14 on universal community service concerning new communication and information services. It is stressed that member States should foster and encourage access for all to Internet communications and information services on a non-discriminatory basis, at an affordable price. In this Declaration, “access for all” is taken to mean access via public access points. Member States may of course go further, if they so wish, by encouraging individual access.

An active participation of the public in the information society, such as setting-up and running individual web sites, should also be encouraged. This means in practice that public authorities should not issue regulations which complicate the setting-up and running of individual web sites, for example licensing or registration systems or any other requirements having a similar effect. A requirement, for instance, to notify the authorities of any changes to a web site might violate this part of the principle.

Principle 5 – Freedom to provide services via the Internet

While Principle 4 deals with access by private persons, Principle 5 focuses on the situation of service providers.

The aim of this principle is to underline that the provision of services via the Internet should not be subject to prior authorisation by the State on the sole ground that this service is provided through the Internet. This is without prejudice to authorisation schemes which govern the provision of services regardless of the means of delivery used (for example, regarding access to certain regulated professions), since these procedures do not address specifically and exclusively the Internet.

This principle is based on Article 4 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter referred to as the "Directive on electronic commerce").

Principle 6 – Limited liability of intermediaries for Internet content

Here it is established that as a general rule intermediaries in the communication chain should not be held liable for content transmitted through their services, except in certain limited circumstances. Along the lines of Articles 12 - 15 of the Directive on electronic commerce, the exemptions to liability take into account the different types of activities of the intermediaries, namely providing access to communication networks, transmitting data and hosting information. The degree of liability depends on the possibilities of service providers to control the content and whether they are aware of its illegal nature. The limitations on liability do not apply if intermediaries intentionally disseminate illegal content.

1st paragraph – no general obligation to monitor

This paragraph is based on Article 15 of the Directive on electronic commerce. Member States should not impose any general obligation on service providers to monitor the information on the Internet to which they give access, that they transmit or store. Nor should they be subject to a general obligation to actively seek facts or circumstances indicating illegal activity, since this might have the effect of curbing freedom of expression.

This paragraph of Principle 6 does not prevent public authorities in member States from obliging service providers in certain cases, for example during a criminal investigation, to monitor the activities of their clients.

2nd paragraph – "mere conduit"

In the case of mere transmission of information or providing access to communication networks, intermediaries should not be held liable for illegal content. When the role of intermediaries goes beyond that, in particular when they initiate the transmission, select the receiver of the transmission or select or modify the information transmitted, their liability may be invoked.

The activity of the intermediary which is at stake here, and which should be exempt from liability, is sometimes referred to as "mere conduit" (cf. Article 12 of the Directive on electronic commerce).

3rd paragraph – "hosting"

In the case of hosting content emanating from third parties, intermediaries should in general not be held liable (cf. Article 14 of the Directive on electronic commerce). This does not apply, however, when the third party is acting under the control of the intermediary, for example when a newspaper company has its own server to host content produced by its journalists. However, if the host becomes aware of the illegal nature of the content on its servers or, in the event of a claim for damages, of facts revealing an illegal activity, it may reasonably be held liable. The precise conditions should be laid down in national law.

4th paragraph – "notice and take down" procedures and freedom of expression and information

As stipulated in paragraph 3 of Principle 6 of the Declaration, service providers may be held liable if they do not act expeditiously to remove or disable access to information or services when they become aware, as defined by national law, of their illegal nature. It is to be expected that member States will define in more detail what level of knowledge is requiredof service providers before they become liable. In this respect, so-called "notice and take down" procedures are very important. Member States should, however, exercise caution imposing liability on service providers for not reacting to such a notice. Questions about whether certain material is illegal are often complicated and best dealt with by the courts. If service providers act too quickly to remove content after a complaint is received, this might be dangerous from the point of view of freedom of expression and information. Perfectly legitimate content might thus be suppressed out of fear of legal liability.

5th paragraph – the possibility of issuing injunctions remains intact

It is highlighted here, in line with Articles 12-14 of the Directive on electronic commerce, that despite the above-mentioned limitations of liability, the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of law, remains intact.

Principle 7 – Anonymity

The aim of this principle is first and foremost to underline that the will of users to remain anonymous should be respected. There are two aspects to this principle. Firstly, users may have a valid reason not to reveal their identity when they have statements published on the Internet. Obliging them to do so could restrict excessively their freedom of expression. It would also deprive society of potentially valuable information and ideas.

Secondly, users need protection against unwarranted on-line surveillance by public or private entities. Member States should therefore, for example, allow the use of anonymity tools or software which enable users to protect themselves.

This principle has, however, its limitations. Member States should have the possibility of obtaining information about persons responsible for illegal activities within the limits laid

down under national law, the Convention for the Protection of Human Rights and Fundamental Freedoms, in particular Article 8, and other relevant international treaties such as the Convention on Cybercrime.