



Ministers' Deputies

CM Documents

CM(2005)56 final 13 May 2005

Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society

The member states of the Council of Europe,

Recalling their commitment to building societies based on the values of human rights, democracy, rule of law, social cohesion, respect for cultural diversity and trust between individuals and between peoples, and their determination to continue honouring this commitment as their countries enter the Information Age;

Respecting the obligations and commitments as undertaken within existing Council of Europe standards and other documents;

Recognising that information and communication technologies (ICTs) are a driving force in building the Information Society and have brought about a convergence of different communication mediums;

Considering the positive contribution the deployment of ICTs makes to economic growth and prosperity as well as labour productivity;

Aware of the profound impact, both positive and negative, that ICTs have on many aspects of human rights;

Aware, in particular, that ICTs have the potential to bring about changes to the social, technological and legal environment in which current human rights instruments were originally developed;

Aware that ICTs are increasingly becoming an integral part of the democratic process;

Recognising that ICTs can offer a wider range of possibilities in exercising human rights;

Recognising therefore that limited or no access to ICTs can deprive individuals of the ability to exercise fully their human rights;

Reaffirming that all rights enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) remain fully valid in the Information Age and should continue to be protected regardless of new technological developments;

Recognising the need to take into account in national legislation new ICT-assisted forms of human rights violations and the fact that ICTs can greatly intensify the impact of such violations;

Conclude that, to better respond to the new challenges of protecting human rights in a rapidly evolving Information Society, member states need to review and, where necessary, adjust the application of human rights instruments;

Undertake to adopt policies for the further development of the Information Society which are compliant with the ECHR and the case-law of the European Court of Human Rights, and which aim to preserve, and whenever possible enhance, democracy, to protect human rights, in particular freedom of expression and information, and to promote respect for the rule of law;

Declare that when circumstances lead to the adoption of measures to curtail the exercise of human rights in the Information Society, in the context of law enforcement or the fight against terrorism, such measures shall comply fully with international human rights standards. These measures must be lawful and defined as precisely as possible, be necessary and proportionate to the aim pursued, and be subject to supervision by an independent authority or judicial review. Further, when such measures fall under the scope of Article 15 of the ECHR, they need to be reassessed on a regular basis with the purpose of lifting them when the circumstances under which they were adopted no longer exist;

Declare that the exercise of the rights and freedoms enshrined in the ECHR shall be secured for all without discrimination, regardless of the technical means employed;

Declare that they seek to abide by the principles and guidelines regarding respect for human rights and the rule of law in the Information Society, found in section I below;

Invite civil society, the private sector and other interested stakeholders to take into account in their work towards an inclusive Information Society for all, the considerations in section II below;

Invite the Chair of the Committee of Ministers to submit this Declaration, as a Council of Europe contribution, to the Tunis Phase of the World Summit on the Information Society (WSIS) for consideration.

I. Human rights in the Information Society

1. The right to freedom of expression, information and communication

ICTs provide unprecedented opportunities for all to enjoy freedom of expression. However, ICTs also pose many serious challenges to that freedom, such as state and private censorship.

Freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10 of the ECHR, simply because communication is carried in digital form.

In guaranteeing freedom of expression, member states should ensure that national legislation to combat illegal content, for example racism, racial discrimination and child pornography, applies equally to offences committed via ICTs.

Member states should maintain and enhance legal and practical measures to prevent state and private censorship. At the same time, member states should ensure compliance with the Additional Protocol to the Convention on Cybercrime and other relevant conventions which criminalise acts of a racist and xenophobic nature committed through computer systems. In that context, member states should promote frameworks for self- and co-regulation by private sector actors (such as the ICT industry, Internet service providers, software manufacturers, content providers and the International Chamber of Commerce). Such frameworks would ensure the protection of freedom of expression and communication.

Member states should promote, through appropriate means, interoperable technical standards in the digital environment, including those for digital broadcasting, that allow citizens the widest possible access to content.

2. The right to respect for private life and correspondence

The large-scale use of personal data, which includes electronic processing, collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission or otherwise, has improved the efficiency of governments and the private sector. Moreover, ICTs, such as Privacy Enhancing Technology (PETs), can be used to protect privacy. Nevertheless, such advances in technology pose serious threats to the right to private life and private correspondence.

Any use of ICTs should respect the right to private life and private correspondence. The latter should not be subject to restrictions other than those provided for in Article 8 of the ECHR, simply because it is carried in digital form. Both the content and traffic data of electronic communications fall under the scope of Article 8 of the ECHR and should not be submitted to restrictions other than those provided for in that provision. Any automatic processing of personal data falls under the scope of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and should respect the provisions of that instrument.

Member states should promote frameworks for self- and co-regulation by private sector actors with a view to protecting the right to respect for private life and private correspondence. A key element of the promotion of such self- or co-regulation should be that any processing of personal data by governments or the private sector should be compatible with the right to respect for private life, and that no exception should exceed those provided for in Article 8, paragraph 2, of the ECHR, or in Article 9, paragraph 2, of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

3. The right to education and the importance of encouraging access to the new information technologies and their use by all without discrimination

New forms of access to information will stimulate wider dissemination of information regarding social, economic and cultural aspects of life, and can bring about greater inclusion and overcome forms of discrimination. E-learning has a great potential for promoting democratic citizenship through education and enhancing the level of people's knowledge throughout the world. At the same time, there is a serious risk of exclusion for the "computer illiterate" and for those without adequate access to information technologies for social, economic or cultural reasons.

Computer literacy is a fundamental prerequisite for access to information, the exercise of cultural rights and the right to education through ICTs. Any regulatory measure on the media and new communication services should respect and, wherever possible, promote the fundamental values of pluralism, cultural and linguistic diversity, and non-discriminatory access to different means of communication.

Member states should facilitate access to ICT devices and promote education to allow all persons, in particular children, to acquire the skills needed to work with a broad range of ICTs and assess critically the quality of information, in particular that which would be harmful to them.

4. The prohibition of slavery and forced labour, and the prohibition of trafficking in human beings

The use of ICTs has expanded the possibilities for trafficking in human beings and has created a new virtual form of this practice.

In a digital environment, such as the Internet, when trafficking in human beings contravenes Article 4 of the ECHR, it should be treated in the same manner as in a non-digital environment.

Member states should maintain and enhance legal and practical measures to prevent and combat ICT-assisted forms of trafficking in human beings.

5. The right to a fair trial and to no punishment without law

ICTs facilitate access to legal material and knowledge. Moreover, public transmission of court proceedings and transparency of information regarding trials facilitates better public scrutiny of court proceedings. Trials can be conducted more efficiently by using ICT-facilities. However, given the speed of ICT-driven communication and the resulting wide-ranging impact, ICTs can greatly intensify pre-trial publicity and influence witnesses and public opinion before and during a trial. Moreover, ICTs allow crimes not covered by legal frameworks, which may hinder combating infringements of human rights. The global reach of ICTs, in particular the Internet, can create problems of jurisdiction and also raise issues on the ability to apply legal frameworks to instances of human rights violation.

In the determination of their civil rights and obligations or any criminal charge against them, everyone is entitled, in conformity with Article 6 of the ECHR, to identical protection in a digital environment, such as the Internet, to that which they would receive in a non-digital environment. The right of no punishment without law applies equally to a digital and a non-digital environment.

Member states should promote codes of conduct for representatives of the media and information service providers, which stress that media reporting on trials should be in conformity with the prescriptions of Article 6 of the ECHR. They should also consider whether there is a need to develop further international legal frameworks on jurisdiction to ensure that the right to no punishment without law is respected in a digital environment.

6. The protection of property

In the ICT environment, the protection of property refers mainly to intellectual property, such as patents, trademarks and copyrights. ICTs provide unprecedented access to material covered by intellectual property rights and opportunities for its exploitation. However, ICTs can facilitate the abuse of intellectual property rights and hinder the prosecution of offenders, due to the speed of technology changes, the low cost of dissemination of content, the volume of infringement, the difficulty in tracking offences across international borders and the decentralised nature of file sharing. Innovation and creativity would be discouraged and investment diminished without effective means of enforcing intellectual property rights.

Intellectual property rights must be protected in a digital environment, in accordance with the provisions of international treaties in the area of intellectual property. At the same time, access to information in the public domain must be protected, and attempts to curtail access and usage rights prevented.

Member states should provide the legal framework necessary for the above-mentioned goals. They should also seek, where possible, to put the political, social services, economic, and research information they produce into the public domain, thereby increasing access to information of vital importance to everyone. In so doing, they should take note of the Council of Europe's Convention on Cybercrime, in particular Article 10, on offences related to infringements of copyright and related rights.

7. The right to free elections

ICTs have the potential, if appropriately used, to strengthen representative democracy by making it easier to hold elections and public consultations which are accessible to all, raise the quality of public deliberation, and enable citizens and civil society to take an active part in policy making at national, regional and local levels. ICTs can make all public services more efficient, responsive, transparent and accountable. At the same time, improper use of ICTs may subvert the principles of universal, equal, free and secret suffrage, as well as create security and reliability problems with regard to some e-voting systems.

E-voting should respect the principles of democratic elections and referendums and be at least as reliable and secure as democratic elections and referendums which do not involve the use of electronic means.

Member states should examine the use of ICTs in fostering democratic processes with a view to strengthening the participation, initiative, knowledge and engagement of citizens, improving the transparency of democratic decision making, the accountability and responsiveness of public authorities, and encouraging public debate and scrutiny of the decision-making process. Where member states use e-voting, they shall take steps to ensure transparency, verifiability and accountability, reliability and security of the e-voting systems, and in general ensure their compatibility with Committee of Ministers' Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting.

8. Freedom of assembly

ICTs bring an additional dimension to the exercise of freedom of assembly and association, thus extending and enriching ways of enjoying these rights in a digital environment. This has crucial implications for the strengthening of civil society, for participation in the associative life at work (trade unions and professional bodies) and in the political sphere, and for the democratic process in general. At the same time, ICTs provide extensive means of monitoring and surveillance of assembly and association in a digital environment, as well as the ability to erect electronic barriers, severely restricting the exercise of these rights.

All groups in society should have the freedom to participate in ICT-assisted associative life as this contributes to the development of a vibrant civil society. This freedom should be respected in a digital environment, such as the Internet, as well as in a non-digital one and should not be subject to restrictions other than those provided for in Article 11 of the ECHR, simply because assembly takes place in digital form.

Member states should adapt their legal frameworks to guarantee freedom of ICT-assisted assembly and take the steps necessary to ensure that monitoring and surveillance of assembly and association in a digital environment does not take place, and that any exceptions to this must comply with those provided for in Article 11, paragraph 2, of the ECHR.

II. A multi-stakeholder governance approach for building the Information Society: the roles and responsibilities of stakeholders

Building an inclusive Information Society, based on respect for human rights and the rule of law, requires new forms of solidarity, partnership and cooperation among governments, civil society, the private sector and international organisations. Through open discussions and exchanges of information worldwide, a multi-stakeholder governance approach will help shape agendas and devise new regulatory and non-regulatory models which will account for challenges and problems arising from the rapid development of the Information Society.

1. Council of Europe member states

Council of Europe member states should promote the opportunities afforded by ICTs for fuller enjoyment of human rights and counteract the threats they pose in this respect, while fully complying with the ECHR. The primary objective of all measures taken should be to extend the benefits of ICTs to everyone, thus encouraging inclusion in the Information Society. This can be done by ensuring effective and equitable access to ICTs, and developing the skills and knowledge necessary to exploit this access, including media education.

The exercise of human rights should be subject to no restrictions other than those provided for in the ECHR or the case law of the European Court of Human Rights, simply because it is conducted in a digital environment. At the same time, determined efforts should be undertaken to protect individuals against new and intensified forms of human rights violations through the use of the ICTs.

Taking full account of the differences between services delivered by different means and people's expectations of these services, member states, with a view to protecting human rights, should promote self- and co-regulation by private sector actors to reduce the availability of illegal and of harmful content and to enable users to protect themselves from both.

2. Civil society

Civil society actors have been and always will be instrumental in shaping the society in which they live, and the Information Society is no exception. To successfully build an Information Society which complies with the standards defined by the ECHR requires the full participation of civil society in both determining strategies and implementing them. Civil society can contribute to developing a common vision for maximising the benefits of ICTs for all and provide its own input into future common regulatory measures that will best promote human rights.

At the Council of Europe, one major channel of civil society input is the Conference of International Non-governmental Organisations (INGOs).

In addition, civil society, in partnership with governments and the business sector, is invited to preserve and enhance its role of drawing attention to and combating the abuse and misuse of ICTs, which are detrimental to both individuals and democratic society in general.

At a trans-national level, civil society is urged to cooperate in the sharing of objectives, best practice and experience with respect to expanding the opportunities held by the Information Society.

3. Private sector

Private sector actors are urged to play a role in upholding and promoting human rights, such as freedom of expression and the respect of human dignity. This role can be fulfilled most effectively in partnership with governments and civil society.

In cooperation with governments and civil society, private sectors actors are urged to take measures to prevent and counteract threats, risks and limitations to human rights posed by the misuse of ICTs or their use for illegal purposes, and to promote e-inclusion. In addition, they are invited to establish and further broaden the scope of codes of conduct and other forms of self-regulation for the promotion of human rights through ICTs.

Private sector actors are also invited to initiate and develop self- and co-regulatory measures on the right to private life and private correspondence, as well as on the issue of upholding freedom of expression and communication.

Self- and co-regulatory measures with regard to private life and private correspondence should emphasise in particular that any processing of personal data should comply with the right to private life. Against this background, private sector actors should pay particular attention to, *inter alia*, the following current issues:

- the collection, processing and monitoring of traffic data;
- the monitoring of private correspondence via e-mail or other forms of electronic communication;
- the right to privacy in the work place;
- camera observation;
- biometric identification;
- malware, including spam;
- the collection and use of genetic data and genetic testing.

With regard to self- and co-regulatory measures which aim to uphold freedom of expression and communication, private sector actors are encouraged to address in a decisive manner the following issues:

- hate speech, racism and xenophobia and incitation to violence in a digital environment such as the Internet;
- private censorship (hidden censorship) by Internet service providers, for example blocking or removing content, on their own initiative or upon the request of a third party;
- the difference between illegal content and harmful content.

Finally, private sector actors are urged to participate in the combat against virtual trafficking of child pornography images and virtual trafficking of human beings.

4. The Council of Europe

The Council of Europe will raise awareness of and promote accession to the Convention on Cybercrime and its Additional Protocol, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, on a worldwide basis. The Convention Committee will monitor the implementation of these conventions and their additional protocols and will, if need be, propose any amendments.

In accordance with the Action Plan adopted by the 7th European Ministerial Conference on Mass Media Policy (Kiev, 10-11 March 2005), the Steering Committee on the Media and New Communications Services (CDMC) will:

- take any necessary initiatives, including the preparation of guidelines, *inter alia*, on the roles and responsibilities of intermediaries and other Internet actors in ensuring freedom of expression and communication;
- promote the adoption by member states of measures to ensure, at the pan-European level, a coherent level of protection for minors against harmful content in traditional and new electronic media, while securing freedom of expression and the free flow of information;
- establish a regular pan-European forum to exchange information and best practice between member states and other stakeholders on measures to promote inclusion in the Information Society;
- monitor the impact of the development of new communication and information services on the protection of copyright and neighbouring rights, so as to take any initiative which might prove necessary to secure this protection.

The objectives of the project "Good governance in the Information Society" will be further defined, taking into account the Council of Europe's work in the fields of e-voting and e-governance, and in particular its achievements represented by Committee of Ministers' Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, and Recommendation Rec(2004)15 on electronic governance ("e-governance").

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) will look into the application of data protection principles to worldwide telecommunication networks.

*Appendix to the Declaration***Council of Europe Reference Texts**

Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

European Convention on Transfrontier Television (ETS No. 132)

Protocol Amending the European Convention on Transfrontier Television (ETS No. 171)

Convention on Information and Legal Co-operation concerning "Information Society Services" (ETS No. 180)

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181)

European Convention for the protection of the Audiovisual Heritage (ETS No. 183)

Protocol to European Convention for the protection of the Audiovisual Heritage, on the protection of Television Productions (ETS No. 184)

Convention on Cybercrime (ETS No. 185)

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)

Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations

Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies

Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunications, with particular reference to telephone service

Resolution ResAP (2001) 3 "Towards full citizenship for persons with disabilities through inclusive new technologies"

Recommendation Rec(2001)7 of the Committee of Ministers to member states on measures to protect copyright and neighbouring rights and combat piracy, especially in the digital environment

Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents

Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting

Recommendation Rec(2004)15 of the Committee of Ministers to member states on electronic governance ("e-governance")

Declaration of the Committee of Ministers on a European policy for New Information Technologies, adopted on 7 May 1999

Declaration of the Committee of Ministers on Cultural Diversity, adopted on 7 December 2000

Declaration of the Committee of Ministers on freedom of communication on the Internet, adopted on 28 May 2003

Political Message from the Committee of Ministers to the World Summit on the Information Society (Geneva, 10-12 December 2003) of 19 June 2003