www.coe.int

COUNCIL CONSEIL
OF EUROPE DE L'EUROPE

Information Documents

SG/Inf(2009)19 **21 October 2009**

_____

Internet - Creating opportunities for all

Document presented by the
Secretary General of the Council of Europe
to the Internet Governance Forum
Sharm El Sheikh, Egypt, 15 – 18 November 2009

_____

Contents

1   Introduction

1.   The World Summit on the Information Society (WSIS, Geneva 2003 – Tunis 2005) reaffirmed, among other things (i) the commitment to build a people-centred, inclusive and development-oriented information society; (ii) the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms; and (iii) determination to strengthen respect for the rule of law in international as in national affairs. It also reaffirmed that democracy, sustainable development and human rights and fundamental freedoms as well as good governance at all levels are interdependent and mutually reinforcing (Tunis Commitment 2005).

2.   Therefore, the Council of Europe (CoE) – as an international organisation which works to promote and protect democracy, human rights and the rule of law – fully supports the Internet Governance Forum (IGF) that was established in 2006 as a result of the WSIS. The IGF is a unique community through which these values, rights and principles can be underscored and reinforced. It offers a platform for dialogue and cooperation in a multi-stakeholder environment. The CoE contributed substantially to the IGF events in Athens (2006) and Rio de Janeiro (2007) and the preparation of the meeting in Hyderabad (2008).

3.   For more than 60 years, the CoE has been developing solutions and responding to issues that have affected policies, legal frameworks and practices in its now 47 member States with more than 800 million people. They are reflected in more than 200 binding treaties[1] and many more recommendations, guidelines and other soft-law instruments. Even if most of these were not developed specifically for the Internet, many of their provisions – including those of the European Convention on Human Rights – apply equally to the online environment.[2] Some – such as the Convention on Cybercrime – are specifically related to information and communication technologies (ICTs). A number of important treaties are open to non-member States.[3] The standards, principles and guidelines of the CoE have therefore been considered "blueprints" by IGF stakeholders.

4.   At the 4th IGF meeting in Sharm El Sheikh, Egypt, from 15 to 18 November 2009, the CoE will again strive to make an important contribution to the overall theme of "Internet – creating opportunities for all" as well as the sub-themes "Security, openness and privacy", "Access and diversity", "Managing critical Internet resources", "Internet governance in the light of WSIS principles" and "Emerging issues: Impact of Social Networks". The present document provides examples of the CoE's work related to these themes and sub-themes.

---

[1] www.conventions.coe.int

[2] The most notable example is the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (often referred to as the European Convention on Human Rights). Using this Convention, ordinary citizens can get redress for human rights violations by applying to the European Court of Human Rights (an institution of the Council of Europe). The case law of the Court contributes to shaping the obligations of states on how rights and freedoms are exercised and protected online.

[3] The Convention on Cybercrime (CETS 185), Convention on the Sexual Exploitation and Abuse of Children (CETS 201) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108) may be particularly relevant in this respect.

2 Internet – creating opportunities for all

5.   In 2007, the CoE's Committee of Ministers adopted a Recommendation on measures to promote the public service value of the Internet. This text explicitly refers to the outcome of the World Summit on the Information Society and underlines the right of everyone to benefit from the information society. It notes that information and communication technologies can significantly enhance the exercise of fundamental rights and freedoms but also points at adverse effects and the need for protective and security measures.

6.   The Recommendation reflects the approach of the CoE with regard to the Internet in a coherent manner, and full implementation of the measures proposed will indeed help ensure that the Internet creates opportunities for all.

Council of Europe Recommendation CM/Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet[4]

I.   Human rights and democracy

Human rights - Member states should adopt or develop policies to preserve and, whenever possible, enhance the protection of human rights and respect for the rule of law in the information society
Democracy[5] - Member states should develop and implement strategies for e-democracy, e-participation and e-government that make effective use of ICTs in democratic process and debate, in relationships between public authorities and civil society, and in the provision of public services as part of an integrated approach that makes full and appropriate use of a number of communication channels, both online and offline

II.   Access - Member states should develop, in cooperation with the private sector and civil society, strategies which promote sustainable economic growth via competitive market structures in order to stimulate investment, particularly from local capital, into critical Internet resources and ICTs, especially in areas with a low communication and information infrastructure

III.   Openness - Member states should affirm freedom of expression and the free circulation of information on the Internet, balancing them, where necessary, with other legitimate rights and interests, in accordance with Article 10, paragraph 2, of the European Convention on Human Rights as interpreted by the European Court of Human Rights

IV.   Diversity - Member states are encouraged to ensure that Internet and ICT content is contributed by all regions, countries and communities so as to ensure over time representation of all peoples, nations, cultures and languages

V.   Security - Member states should engage in international legal cooperation as a means of developing and strengthening security on the Internet and observance of international law

---

[4] Available at:
http://wcd.coe.int/ViewDoc.jsp?id=1207291&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

[5] For a more detailed set of principles and guidelines on e-democracy, see Recommendation CM/Rec(2009)1 of the Committee of Ministers to member states on electronic democracy (e-democracy), available at: https://wcd.coe.int/ViewDoc.jsp?id=1410627&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

3 Security, openness and privacy

7.   Security, privacy and openness on the Internet are mutually reinforcing pre-conditions for users to be able to freely express themselves and to access information. By stepping up levels of user security and privacy their confidence to use the Internet will grow. On this basis, the Internet is becoming an essential tool for everyday activities (communication, information, knowledge, commercial transactions, and entertainment). There will be a greater demand for Internet services and, as a corollary, there will be a greater legitimate expectation that such services will be *inter alia* secure and reliable.

3.1 Reinforcing human rights

8.   According to the above-mentioned Recommendation on measures to promote the public service value of the Internet, states should adopt or develop policies to preserve and, whenever possible, enhance the protection of human rights and respect for the rule of law in the information society. In this regard, particular attention should be paid to:

-    the right to freedom of expression, information and communication on the Internet and via other ICTs
-    the right to private life and private correspondence on the Internet
-    the right to education, including media and information literacy
-    the fundamental values of pluralism, cultural and linguistic diversity, and non-discriminatory access to different means of communication via the Internet and other ICTs
-    the dignity and integrity of the human being with regard to the trafficking of human beings carried out using ICTs and by signing and ratifying the CoE Convention on Action against Trafficking in Human Beings (CETS No. 197)
-    the right to the presumption of innocence, the right to a fair trial and the right to no punishment without law in the digital environment
-    the freedom for all groups of society to participate in ICT-assisted assemblies and other forms of associative life
-    the right to property, including intellectual property rights, subject to the right of the state to limit the use of property in accordance with the general interest.

Freedom of expression and freedom of the media on the Internet

9.   The Internet is having a significant impact on the way in which information is gathered, content is created as well as on the methods by which both are made available and sought. This was a central theme of the 1st CoE Conference of Ministers responsible for media and new communication services, held in Reykjavik on 28 and 29 May 2009. The ministers stated (in their Resolution *Towards a new notion of media*) that new media and media-like mass communication services fulfil some of the functions so far carried out by 'traditional media'. They underlined that fundamental rights and freedoms, including the freedom of the media, have to be promoted and protected regardless of these changes.

10.   The CoE has therefore started to review the concept of media itself and is examining criteria to distinguish media or media-like services from new forms of personal communication. This is because the exercise of freedom of expression and information also carries with it duties and responsibilities. The ministers underlined that media and media-like providers have to respect certain benchmarks and should be adequately informed of

their responsibilities. The CoE will continue to develop such benchmarks together with all relevant stakeholders.

11.   For many people, the right and freedom to receive and impart information and ideas on the Internet is becoming a necessity rather than a choice for economic, financial and social reasons. As reliance and dependency on the Internet grows, this right and freedom becomes even more important. Fostering trust and confidence on the Internet is therefore crucial to the Internet's openness.

Human rights cooperation and capacity building with the private sector

-       Human rights guidelines for Internet service providers[6]
-       Human rights guidelines for online games providers[7]

12.   Raising awareness of and promoting respect for human rights in the creation, development and provision of Internet services and technologies is also central to discussions regarding security, openness and privacy. The CoE is currently working on standards concerning the rights and responsibilities of users with regard to data retention, processing of personal data and profiling techniques or practices.

13.   The CoE's human rights guidelines for Internet service providers and for online games providers[8] are acknowledged by the industry bodies – European Internet Services Providers Association (EuroISPA) and the Interactive Software Federation of Europe (ISFE) – as being more effective than (government) rules and regulations. They believe that the guidelines provide a flexible and dynamic means of establishing cooperation and dialogue between different stakeholder groups including the private sector and governments. They also consider the guidelines to be a source of reference or inspiration in the process of content creation or distribution, and a unique tool for awareness raising.[1]

---

[6] Available at http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf

[7] Available at http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)008_en.pdf;

[8] Human rights guidelines for online games providers available at:
 http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)008_en.pdf;
Human rights guidelines for Internet service providers available at:
 http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf
These guidelines were prepared and launched in 2008 in close cooperation with the European Internet
Service Providers Association (EuroISPA) and the Interactive Software Federation of Europe (ISFE).

3.2 Protecting children's dignity, security and privacy on the Internet

14.   Fostering children's trust and confidence in the Internet coupled with the protection of their dignity, security and privacy is a priority for the CoE. The Internet is a space of freedom to express and to communicate, to search for information and to learn, to work and to play. Access to the Internet thus offers great potential for children to exercise and enjoy their rights and values through the Internet.

15.   At the same time, threats such as cybercrime and the sexual exploitation and abuse of children through information and communication technologies pose particular challenges. The CoE is addressing these by setting common standards and policies, by supporting educational, preventive and other measures to empower children, by promoting criminal justice action and by strengthening multi-stakeholder and international cooperation.

16.   CoE standards as regards the protection of children and promotion of their rights include numerous treaties and recommendations, some of which are specifically related to the online environment.

- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)
- Convention on Cybercrime (CETS 185)
- Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment[9]
- Declaration on protecting the dignity, security and privacy of children on the Internet, adopted by the Committee of Ministers on 20 February 2008[10]
- Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, adopted on 8 July 2009[11]
- Parliamentary Assembly Recommendation 1882 (2009) on the promotion of Internet and online media services appropriate for minors.[12]

The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)[13]

17.   The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) represents the most advanced and comprehensive standard in this field. A body to monitor compliance with this treaty is envisaged to be set up in 2010. The Convention provides for:

---

[9]

https://wcd.coe.int/ViewDoc.jsp?Ref=Rec(2006)12&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75
[10]

https://wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75
[11]

https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2009)5&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

[12] http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1882.htm

[13] www.conventions.coe.int

- the criminalisation of sexual abuse of children, child prostitution, child pornography, grooming and other conduct
- preventive measures, including education of children on the risks of sexual exploitation and abuse through the use of new information technologies
- assistance to victims
- the participation of children, the private sector, the media and civil society in measures to protect children and prevent their abuse
- holding nationals accountable for offences committed abroad
- the protection of children in the course of criminal proceedings
- international cooperation.

18.   Children of increasingly young ages are taking part in social networking websites and chatrooms and expose themselves to the risk of being groomed for sexual purposes. In very few states is the conduct of grooming a criminal offence. The CoE has contributed to closing this legal loophole in the Convention by making it an offence for an adult to arrange to meet a child through information and communication technologies with the intention of engaging in unlawful sexual activities with the child.

19.   The Convention contains many references to the use of information and communication technologies in the context of the sexual exploitation and sexual abuse of children. For example, it requires states to criminalise conduct such as knowingly accessing child pornography on the Internet. This treaty and the Convention on Cybercrime thus complement each other.

20.   Broadest possible implementation of this treaty together with the Convention on Cybercrime is recommended as effective means to protect children against sexual exploitation and abuse and to hold offenders accountable.

The Convention on Cybercrime (CETS 185)[14]

21.   The "Budapest" Convention on Cybercrime (CETS 185) is the global standard on cybercrime. The implementation of the Convention is followed by the Cybercrime Convention Committee (T-CY), which is also responsible for dealing with policy issues and legal questions arising from the practical cooperation under this instrument. The Convention stipulates that state parties:

- criminalise offences against and through computer systems. Article 9 covers child pornography in a broad manner
- introduce procedural law measures to provide law enforcement with effective means to investigate cybercrime including child pornography and the sexual exploitation and abuse of children related to computer systems
- cooperate efficiently with each other and provide a framework for international cooperation, including police and judicial cooperation in computer-related cases involving crimes against children.

---

[14] www.coe.int/cybercrime

Educative and preventive measures and empowering children[15]

22.   The 3rd Summit of Heads of State and Government of the Council of Europe (Warsaw 2005), among other things, led to the launch of the programme "Building a Europe for and with Children". This programme aims at promoting the rights of children as well as their protection against all forms of violence. It is built on the four "P's" of prevention, prosecution, protection and participation. Among the preventive measures related to the new media are an online Internet safety game for children ("Through the Wild Web Woods") and an Internet Literacy Handbook.[16] Available in 24 languages, the game has been played by over 2.4 million children and adults across Europe. The game is now accompanied by a Teachers' Guide offering model lessons on issues, such as online identity, addiction, privacy, and children's rights in real and virtual worlds.

"*Through the Wild Web Woods*"[17] is an online game designed by the CoE which helps children learn basic Internet safety rules. The game uses familiar fairy tales to guide children through a maze of potential dangers on the way to the fabulous e-city Kometa, while teaching them to protect identity and personal data, participate safely in chat rooms, recognise sites and online games containing dangerous or harmful content, develop critical approach towards information found on the Internet, and protect their computers against spam and viruses. The game also promotes such key concepts and values underlying the work of the CoE, as democracy, respect for others and children's rights.

The game, mainly for children between 7 and 10, is now available in 24 languages. It is accompanied by an online teaching guide proposing structural ways for teachers to discover Internet safety together with the kids.

---

23.   Through its Stockholm strategy 2009 – 2011, the CoE is supporting the implementation of national strategies on the protection of children from violence. For autumn 2010, a Europe-wide campaign against sexual violence against children is planned with a particular reference to the new media.

24.   The CoE furthermore recommends that:

-    Children are empowered so that they can acquire the necessary skills to create, produce and distribute content and communications to help them exercise and enjoy their rights and freedoms, especially the right to freedom of expression and information. This is why the Committee of Ministers recommends (in its Recommendation (2006)12) that member states ensure children become familiar with, and skilled in, the new information and communications environment and that, to this end, information literacy and training for children become an integral part of school education from an early stage in their lives.

-    Children have the confidence and trust online by being able to use "islands of trust" otherwise known as "walled gardens" in which they explore, learn and play. This is why the Committee of Ministers adopted Recommendation (2009)5 so that public-private partnerships are encouraged to (i) create and facilitate confidence building environments (walled gardens) for children to safely explore the Internet, (ii) create a

---

[15] www.coe.int/children

[16] http://www.coe.int/t/transversalprojects/children/publications/internetliteracy_en.asp

[17] http://www.wildwebwoods.org/popup_langSelection.php

human rights based pan-European trustmark which harnesses new and existing online content labeling systems, and (iii) improve children's media literacy.

- Children's dignity, security and privacy on the Internet is strengthened and developed, in particular so that there are no lasting or permanently accessible records of the content created by children on the Internet which challenges their dignity, security and privacy or otherwise renders them vulnerable now or at a later stage in their lives.

- Children have access to filters which are age appropriate and "intelligent" as a means of encouraging access to and confident use of the Internet and are a complement to other strategies on how to tackle harmful content. In this connection, the use of such filters should be proportionate and should not lead to the overprotection of children.

25.   The CoE Parliamentary Assembly Recommendation 1882 (2009)[18] on the promotion of Internet and online media services appropriate for minors outlines a number of policy guidelines, such as (i) to encourage public or private educational institutions, museums, orchestras and other cultural institutions as well as public service broadcasters to provide Internet and online content for children and adolescents, (ii) to ensure that access to adult content is effectively restricted by age-verification systems installed by the providers of such content, (iii) to analyse the potential psychological risks for children and adolescents using Internet and online media excessively, in particular social online networks suggesting virtual reality as well as violent online games and networks, and (iv) to initiate an international campaign aimed at accession to the Convention on Cybercrime also by states outside Europe, in order to cover better the world wide map of cyberspace and avoid geographical loopholes.

26.   The CoE Parliamentary Assembly believes that it will be helpful, especially with regard to minors, to develop secure and restricted computer networks often referred to as Intranets, walled gardens or gated communities, which are accessible to an identifiable group of users only, typically require adherence to a code of conduct, fall under a clear set of legal rules and the jurisdiction of a given country, and filter content harmful to minors. The Assembly also appeals to the online media industry to develop and apply codes of conduct with regard to privacy protection, equal opportunities, commercial activities targeted at minors and content potentially harmful to them. Internet hotlines and other complaint mechanisms against potentially illegal and harmful content or conduct should be maintained by Internet service and content providers. Commercial services provided in conformity with high ethical standards and high safety protection for minors will be in growing demand in an ever expanding Internet and online media market.

---

[18]   http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1882.htm

3.3 Protection of personal data and privacy

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108)[19]
- Additional Protocol on supervisory authorities and transborder data flows (CETS 181)
- Recommendations on data protection in different sectors[20]
- Recommendation on profiling (in preparation)

27.   According to Article 8 of the European Convention on Human Rights, everyone has the right to respect for his private and family life, his home and his correspondence. Privacy is more than the right to be left alone. Data protection is essential for the development and fulfillment of one's personality. It is a condition for self-determination and for protecting the freedom of expression and human dignity, for preventing control and manipulation and thus a precondition for freedom and democracy.

28.   The Internet poses serious risks to privacy and the protection of personal data and enables intrusive practices into people's privacy. It is possible to record and store virtually every online activity of Internet users for an indefinite period of time. Often, users are not aware of the large amount of personal data about them on the Internet.

29.   New technologies and developments such as cloud computing, IPv6 or the interoperability of devices, and the trend towards the authentication of users and machines to enhance security will increase risks to privacy.

30.   In order to provide effective personal data protection it is vital to strengthen laws and practices so that privacy-compliant practices can spread on the Internet and foster users' trust in the processing of their data. As transborder data flows are an intrinsic feature of the Internet, it is essential to take measures to protect personal data at a global level.

31.   The CoE's guidelines on the public service value of the Internet[21] recommend that states improve their domestic frameworks for privacy law in accordance with Article 8 of the European Convention on Human Rights and by signing and ratifying the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108), that they provide for appropriate safeguards for the transfer of international personal data to states which do not have an adequate level of data protection, and that they facilitate cross-border cooperation in privacy law enforcement.

32.   The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108) and its Additional Protocol on supervisory authorities and

---

[19] See http://www.conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG

[20]

http://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/instruments%20juridiques%20internationaux/12Recommandations%20et%20resolutions%20du%20Comite%20des%20Ministres_fr.asp#TopOfPage

[21] Council of Europe Recommendation CM/Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet:
http://wcd.coe.int/ViewDoc.jsp?id=1207291&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

transborder data flows (CETS 181) contain minimum standards for personal data protection. These instruments aim at protecting individuals against infringement of their privacy and the misuse of personal data and, at the same time, offer a well established framework for the exchange of personal data, mutual assistance and a forum for the development of new standards.

33.   The Convention has a global vocation and is open for accession by non-European countries. On 2 July 2008, the Committee of Minister of the CoE adopted a decision encouraging non-member states to consider accession to Convention 108. The worldwide promotion of this treaty was launched by the CoE with a view to reinforcing the global nature of the right to privacy and personal data protection in today's world of borderless communication networks.

34.   The Consultative Committee of the Convention (T-PD) is a body that monitors the implementation of the Convention and is also engaged in standard-setting work, the drafting of legal instruments that allow enhancing data protection and adapting the Convention's provisions to specific sectors or technologies. The CoE has adopted 13 sectoral recommendations concerning, inter alia, direct marketing, social security, police, telecommunications, medical data and the protection of privacy on the Internet. These have been supplemented by other texts such as the Guide to the preparation of contractual clauses, guiding principles on video surveillance and on smart card and a progress report on biometric data.

35.   The increasing development of new information and communication technologies which allow routine online collection and matching of personal data on a large scale and subsequent various use of it, in particular, for producing profiles and their application to individuals led to the Committee of Ministers' decision to prepare a draft Recommendation on Profiling. This document is focusing on the condition of collection and processing of personal data using profiling such as lawfulness, duty of information, right to object. Its aim is striking the right balance between the rights of data subject and online advertising interests. It will assist states in improving the protection of individuals against abusive use of profiles.

36.   Efficient protection of privacy in the online world cannot be envisaged without close cooperation with the private sector and the promotion of self-regulation mechanisms such as codes of conduct as well as the development of privacy enhancing technologies. The benefits of technological enhancements must be shared among all stakeholders of the e-society. It is important to have a legal framework to keep control over the technological evolution so that the technological progress will not undermine human rights.

37.   While Assembly Recommendation 1882 (2009)[22] on the promotion of Internet and online media services appropriate for minors calls on the online media industry to develop and apply codes of conduct with regard to privacy protection, a new initiative of the CoE's Parliamentary Assembly will analyse policies on "privacy and the management of private information on the Internet and other online media".[23]

38.   Individuals should be able to determine themselves the management of their private information on the Internet and online media. Therefore, it is necessary for states to assess

---

[22]   http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1882.htm

[23]   http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc09/EDOC12021.htm

this objective and provide adequate means to fulfil it. Technological means, greater user awareness, self-regulatory standards – for instance by the Internet industry and employers, as well as legal instruments should be evaluated in this respect.

3.4 Meeting the challenge of cybercrime[24]

- "Budapest" Convention on Cybercrime (CETS 185)
- Protocol on Xenophobia and Racism committed through Computer Systems (CETS 189)
- Global Project on Cybercrime for technical assistance
- Guidelines for law enforcement – ISP cooperation in the investigation of cybercrime
- Concept for cybercrime training of judges and prosecutors[25]

39. Cybercrime is posing an increasing threat to societies that rely on information and communication technologies. The CoE helps countries address this challenge in particular through the Convention on Cybercrime and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobia nature through computer systems.

40. The Convention on Cybercrime (CETS 185) provides for (i) the criminalisation of conduct – ranging from illegal access, data and systems interference to computer-related fraud and child pornography; (ii) tools to make the investigation of cybercrime more effective and (iii) efficient international cooperation. It is the only binding treaty on this matter in the world and open for accession by any country.

41. The Convention is supplemented by an Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189).

42. The Cybercrime Convention Committee (T-CY) monitors the implementation of the Convention and its Protocol and is also responsible for dealing with policy issues and legal questions arising from cooperation under these instruments.

43. In addition, the CoE Project on Cybercrime cooperates with a wide range of partner organisations representing both industry and civil society and provides specific support to countries by:

- encouraging states across the world to use the Convention on Cybercrime as a "model law" when developing national legislation
- assisting states when elaborating legislation and preparing to sign, ratify or accede to the Cybercrime Convention
- encouraging states to fully cooperate at international level against cybercrime through the framework provided by the Convention
- helping law enforcement authorities and Internet service providers to work together by using the Council's guidelines on cooperation as a means to structure and organise their cooperation when investigating cybercrime[26]
- developing methodologies and delivering training for judges, prosecutors and law enforcement[27]

---

[24] See www.coe.int/cybercrime

[25] Available at www.coe.int/cybercrime

[26] Guidelines for the cooperation between law enforcement authorities and ISPs (April 2008)

- facilitating action against criminal money flows on the Internet[28]
- helping countries address issues related to cybercrime such as the protection of children and personal data.

44.   The CoE is cooperating with a wide range of public and private sector partners and international organisations to create synergies, promote convergence and provide best possible support and guidance to states worldwide.

45.   It is essential that all partners engage in a cooperative effort and provide clear guidance to countries worldwide by making use of existing instruments. By mid-2009, more than 100 countries from all continents have been using the Convention on Cybercrime as a guideline or reference when developing new legislation or reviewing and improving existing laws related to cybercrime. In addition to member States of the CoE several other countries have signed (Canada, Japan, South Africa) or ratified (United States of America) this treaty or have been invited to accede (Chile, Costa Rica, Dominican Republic, Mexico, Philippines), and the accession by other countries is under consideration. There is thus a global trend towards the strengthening of cybercrime legislation in a harmonised manner on the basis of this Convention.

46.   The CoE Parliamentary Assembly has called for an international campaign aimed at the accession also by non-European countries to the Convention on Cybercrime in order to enlarge geographical coverage and avoid loopholes.[29]

3.5 Countering the terrorist use of the Internet[30]

-    Convention on the Prevention of Terrorism (CETS 196)
-    "Budapest" Convention on Cybercrime (CETS 185)

47.   The CoE has drawn up several innovative international treaties addressing terrorism, some as early as the 1970s. More recently, in 2005, the Convention on the Prevention of Terrorism[31] was adopted which, like the Convention on Cybercrime has a global application and has received considerable international support; it is regarded as a precursor to certain developments at global level, notably to the adoption by the United Nations Security Council of Resolution 1624 in September 2005.

48.   This treaty is the first to require that states establish as criminal offences conduct that may lead to the commission of acts of terrorism, including public provocation or

---

[27] A Concept for the training of judges and prosecutors in matters related to cybercrime and electronic evidence was prepared under the Project on Cybercrime and adopted by the CoE's Lisbon Network of Judicial training institutions in September 2009 (available at www.coe.int/cybercrime)

[28] In September 2009, the CoE's anti-money laundering monitoring mechanism MONEYVAL decided to undertake a typology exercise in criminal money flows on the Internet in cooperation with the Project on Cybercrime

[29]   http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1882.htm

[30] Council of Europe theme file on Terrorism: the worst enemy of democracy: http://www.coe.int/t/dc/files/themes/terrorisme/default_en.asp

[31] The Council of Europe Convention on the Prevention of Terrorism (CETS 196) entered into force on 1 June 2007 and to date, it has been signed by 32 and ratified by 7 Council of Europe member States http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=1&DF=13/10/2009&CL=ENG

indirect incitement, recruitment and training for terrorist purposes. The Convention applies, for example, to the glorification and justification of terrorism and terrorist acts, recruitment for terrorism and to terrorist training carried out by using the Internet or other electronic communication systems. The Convention also requires that the establishment, implementation and application of the pertinent criminal law provisions respect human rights obligations, in particular the rights to freedom of expression, association and religion. As a result, the Convention has been characterised as "a sound response which would respect human rights".[32]

49.   If the CoE Convention on the Prevention of Terrorism effectively addresses the Internet *as a means,* the question then arises: what about the Internet and other electronic communication systems *as a target* of cyber attacks by terrorists? Examples of massive attacks on private and national Internet resources already exist and international community should prepare for the growing cyber capabilities of terrorists in addition to the threats posed by cyber criminals and other such actors.

50.   There is a growing consensus that the combined effect of the Convention on Cybercrime and its Additional Protocol, and the CoE Convention on the Prevention of Terrorism allows states to respond adequately to Internet security challenges. The CoE will continue to promote a widespread adherence to these instruments as a basis for international cooperation in countering the terrorist use of the Internet.

51.   The Parliamentary Assembly of the CoE in its Recommendation 1706 (2005)[33] proposed the setting up a framework for security cooperation between member and observer states for the prevention of cyber terrorism, in the form of large-scale attacks on and through computer systems which threaten a state's national security, public safety or economic well-being.

3.6 Medicines on the net – risks and benefits

-    Council of Europe Convention against counterfeiting of medical products and similar crimes involving threats to public health [in preparation]
-    Resolution ResAP(2007)2 on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine[34]

52.   The CoE promotes the fundamental right of citizens to have access to information on health issues. The global nature of the Internet makes it an excellent medium to promote health literacy but also to publish misleading information or to market harmful healthcare products. Consumers perceive convenience in buying medicines and healthcare products via the Internet. There are countless illegal offers of medicines via the Internet, many of them

---

[32] See Report of Martin Scheinin, United Nations Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism, E/CN.4/2006/98, para. 56 (c), available at http://daccessdds.un.org/doc/UNDOC/GEN/G05/168/84/PDF/G0516884.pdf?OpenElement This position was also underlined in the Report of the Counter-Terrorism Committee to the Security Council on the implementation of Resolution 1624(2005).

[33]   http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta05/EREC1706.htm
[34]
   http://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

counterfeit.[35] Often, Internet users are not aware of or do not know how to avoid the risks posed by illegal offers on the web. This may result in serious damage to health, financial loss, fraud and cybercrime.

53.   The European Directorate for the Quality of Medicines & HealthCare (EDQM) contributes to the basic human right of access to good quality medicines and healthcare, and promotes and protects human and animal health through standard-setting, assistance for and coordination of implementation, and the development of policies and model approaches.

54.   Action against the threat of counterfeit and illegal medicines and healthcare products offered on the web is taken by:

-    preparing an international legal instrument, a CoE Convention against counterfeiting of medical products and similar crimes involving threats to public health. This treaty is expected to be opened for signature in 2010

-    setting standards on good practices for distributing medicines via mail order which facilitates the protection of patient safety and the quality of delivered medicine[36]

-    implementing special work programmes to protect public health from counterfeit medicines and similar crimes (e.g. risk management and prevention strategies, model approaches for multi-disciplinary cooperation, knowledge building, and regular training)[37].

55.   The focus of the future Convention[38] is on the threat to public health and not on intellectual property rights. The following intentional acts will be criminalised:

-    the manufacturing of counterfeits
-    the supplying or offering to supply of, and trafficking in counterfeits
-    the falsification of documents
-    the unauthorised manufacturing or supplying of medicinal products and the placing on the market of medical devices without them being in compliance with the conformity requirements.

56.   The future Convention also provides a framework for international cooperation, measures for co-ordination at national level, preventive measures and protection of victims and witnesses. The future Convention, the first international binding treaty in this field is to be open for participation by any country, and could thus provide a global criminal law framework against a global threat.

---

[35] Medicines purchased over the Internet from sites that conceal their physical address are counterfeit in over 50% of cases (WHO). Up to 20% of medicines traded via Internet in the USA and Canada is assumed to be counterfeit.

[36] Council of Europe Resolution ResAP(2007)2 of the Committee of Ministers on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine:
http://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

[37] http://www.edqm.eu/en/Pharmaceuticals_Pharmaceutical_care-1271.html
[38] http://www.coe.int/t/dghl/standardsetting/pharmacrime/default_EN.asp?

4 Access and diversity

57.   Access to Internet services concerns the enjoyment of human rights and fundamental freedoms, as well as the exercise of democratic citizenship. This was underlined by the ministers participating in the 1st CoE Conference of Ministers responsible for media and new communication services, held in Reykjavik on 28 and 29 May 2009. In particular, the ministers declared:

> "Growing numbers of people rely on the Internet as an essential tool for everyday activities (communication, information, knowledge, commercial transactions, leisure), ultimately improving their quality of life and well-being. People therefore expect Internet services to be accessible and affordable, secure, reliable and ongoing."[39]

4.1 Access and diversity: the public service value

58.   Access and diversity are not aims in themselves. Access and diversity are important for democracy and human rights because they ensure the individual's right to information and participation in political, social, cultural and economic life. This information has to be trustworthy. In the Resolution *Towards a new notion of media,* adopted at the above-mentioned conference, the ministers identified a number of risks to access and diversity of trustworthy content:

> "Individuals' right to receive information can be challenged and democracy can be threatened by negative and significant market distortion as a result of media concentration; lack of diversity and pluralism; manipulative messages; new forms of content aggregation; the management and prioritisation of flow of content and of access and limited connectivity, or lack of access, to broadband services."

59.   These risks can be mitigated by states through recognition of the public service value of the Internet and promotion of genuine, independent and adequately resourced public service media as a means of providing trustworthy and diverse information to all segments of society.[40] As a result, exploring new approaches to the governance of public service media (on- and offline) to ensure people's full participation in political, social and cultural life[41] and examining to which extent universal access to the Internet should be developed as part of member states' provision of public services[42] is a priority for the CoE.

---

[39] For this and other references to the various documents adopted at the 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services A new notion of media? (28 and 29 May 2009, Reykjavik, Iceland) *Political declaration and resolutions* see:
 http://www.coe.int/t/dghl/standardsetting/media/MCM(2009)011_en_final_web.pdf and
 www.ministerialconference.is

[40] In this context see Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet: available at:
https://wcd.coe.int/ViewDoc.jsp?id=1207291&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

[41] For the Terms of Reference of the Ad-hoc Advisory Group on Public Service Media Governance, consult
http://www.coe.int/t/dghl/standardsetting/media/MC-S-PG/MC-S-PG_mandat_en.asp#TopOfPage

[42] This may include policies for redressing market failure where market forces are unable to satisfy all legitimate needs or aspirations, both in terms of infrastructure and the range and quality of available content and services.

60.   Measures proposed in the CoE Recommendation on the public service value of the Internet[43] include that states – in cooperation with the private sector and civil society – should develop strategies aimed at promoting:

-    affordable access to ICT infrastructure, including the Internet
-    technical interoperability, open standards and cultural diversity in ICT policy covering telecommunications, broadcasting and the Internet
-    diversity of software models, including proprietary, free and open source software
-    affordable access to the Internet for individuals, irrespective of their age, gender, ethnic or social origin, including persons and groups of persons on low income, in rural and geographically remote areas, and with special needs (for example, disabled persons)
-    a minimum number of Internet access points and ICT services on the premises of public authorities and, where appropriate, in other public places
-    public administrations, educational institutions and private owners of access facilities to new communication and information services to enable the general public to use these facilities.

61.   In terms of diversity, the same Recommendation encourages states "to ensure that Internet and ICT content is contributed by all regions, countries and communities so as to ensure over time representation of all peoples, nations, cultures and languages". A number of specific measures proposed include promoting digital content production by national or local cultural industries, preserving the digital heritage of lasting cultural, scientific, or other values, encouraging access to educational, cultural and scientific content in digital form, so as to ensure that all cultures can express themselves and have access to the Internet in all languages, including indigenous ones, encouraging capacity building for the production of local and indigenous content on the Internet, and encouraging the multilingualisation of the Internet so that everyone can use it in their own language.

62.   The Parliamentary Assembly endorsed this approach to the Internet with regard to audiovisual media services in its Recommendation 1855 (2009)[44]. Based on traditional universal service requirements of telecommunications as well as the notion of public service broadcasting, Internet-based audiovisual media services will have an essential function for society and each individual.

63.   While Article 10, paragraph 1, of the European Convention on Human Rights[45] permits states to require "the licensing of broadcasting, television or cinema enterprises", the CoE Parliamentary Assembly believes that broadcasting and television in this sense should not include Internet radio or web television, which should not require national authorisations. Internet radio and web television should be treated like Internet-based newspapers or websites with text, images and sound.[46]

---

[43] Available at:
http://wcd.coe.int/ViewDoc.jsp?id=1207291&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75
[44]   http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1855.htm
[45]   http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm
[46]   http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1855.htm   [see §4 of Assembly Recommendation 1855 (2009)]

4.2 Access for people with disabilities

64.   The right and freedom to receive and impart information should also be considered from the disability perspective: is the information accessible for people with disabilities in form and content? Are people with disabilities able to participate in and contribute to public debates via Internet? Does the Internet help improve the quality of life of people with disabilities by contributing to a greater access to and active participation in education, employment, culture, tourism or politics?

65.   The CoE Report "Achieving full participation through Universal Design"[47], published in April 2009, contains various examples of good practices in member states on how the design and provision of information and communication technology can help improve the quality of life of people with disabilities.

66.   In May 2009, the European Co-ordination Forum for the Council of Europe Disability Action Plan 2006-2015[48] tabled a position paper[49] at the Conference of Ministers responsible for media and new communication services, stressing that "media and new communication services have the capacity and responsibility of contributing to an environment that is conducive to the full integration and active participation of people with disabilities in society, in particular people with sensorial or intellectual impairments and learning difficulties".[50]

67.   The newly created Committee of Experts on participation of people with disabilities in political and public life, set up to take stock of the current situation in Europe[51] and to draft recommendations for all CoE member states by 2011, will address the issue of Internet accessibility in the context of e-voting and e-governance.

4.3 Participation by children

68.   Listening to children and taking their opinion into account in all decisions concerning them is an inherent children's human right protected by the UN Convention on the Rights of the Child. Children are competent in a variety of issues, and their evolving capacity enables them to form views on many relevant subjects.

69.   Measures proposed in the CoE Recommendation on the public service value of the Internet[52] include the integration of ICTs into education, and promoting media and

---

[47] Achieving full participation through Universal Design, Council of Europe Publishing, Strasbourg, April 2009, ISBN 978-92-871-6474-2.

[48] Recommendation Rec(2006)5 of the Committee of Ministers to the member States on the Council of Europe Action Plan to promote the rights and full participation of people with disabilities in society: improving the quality of life of people with disabilities in Europe 2006-2015

[49] CAHPAH-T(2008)7 final, Position Paper, CAHPAH Rapporteur: Mr Dany Dewulf, Belgium

[50] 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services A new notion of media? (28 and 29 May 2009, Reykjavik, Iceland):
http://www.coe.int/t/dghl/standardsetting/media/MCM(2009)011_en_final_web.pdf and
www.ministerialconference.is

[51] Follow-up to Action Line 1 of the Council of Europe Disability Action Plan 2006-2015 and Article 29 of the United Nations Convention on the Rights of Persons with Disabilities

[52] Available at:
http://wcd.coe.int/ViewDoc.jsp?id=1207291&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

information literacy and training in formal and non-formal education sectors for children and adults in order to:

- empower them to use media technologies effectively to create, access, store, retrieve and share content to meet their individual and community needs and interests
- encourage them to exercise their democratic rights and civic responsibilities effectively
- encourage them to make informed choices when using the Internet and other ICTs by using and referring to diverse media forms and content from different cultural and institutional sources; understanding how and why media content is produced; critically analysing the techniques, language and conventions used by the media and the messages they convey; and identifying media content and services that may be unsolicited, offensive or harmful.

70. Internet provides plenty of opportunities for children's e-participation at local, national, European and global levels. At the local level, the 2008 CoE Congress of Local and Regional Authorities Recommendation on Electronic democracy and deliberative consultation on urban projects encourages e-participatory initiatives with the involvement of young persons to discuss sustainable urban planning, spatial development and local infrastructure facilities.

71. At national and European level, a pilot project currently developed by the "Building a Europe for and with children" programme will allow the setting up of a laboratory on child participation exploring *inter alia* the role of information and communication technologies in this respect. The possibility of children contribution to CoE deliberations is also on the agenda.

4.4 E-learning

72. New communication services offer, for instance, better opportunities for e-learning. The CoE Parliamentary Assembly calls on states in its Recommendation 1836 (2008) [53] to realise the full potential of e-learning for education and training. In an era of globalisation and rapid technological change, a state's competitiveness and wealth will depend on its ability to become an advanced, knowledge-based society through constant improvement in lifelong education and training of the population in general and the workforce in particular. Therefore, states should supplement traditional classroom-based school education by e-learning. E-learning can also be more inclusive, in particular for people with disabilities and the socially challenged. E-learning can be a powerful means of creating open educational resources accessible to everybody.

4.5 Interoperability of technical standards

73. Access requires also interoperability of technical standards and availability of technical means such as radio-frequencies. On both issues, the CoE Parliamentary Assembly Recommendation 1855 (2009)[54] invites member States of the International Telecommunication Union of the United Nations to "advance international co-ordination of the technological standards necessary for the technological convergence of audiovisual media, while ensuring the right to freedom of information regardless of frontiers under

---

[53] http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta08/EREC1836.htm

[54]   http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1855.htm

Article 19 of the International Covenant on Civil and Political Rights" and "prepare for the World Radiocommunication Conference in 2011 decisions on the allocation of radio-frequency spectrum following the analogue switch-off of broadcasting in many countries." When deciding on the allocation of the radio-frequency spectrum, states should also balance the spectrum needs of various technologies relating to both broadcasting and telecommunications. It will be particularly relevant to look at the availability of the spectrum for all countries and how spectrum resources can be allocated to optimise opportunities for public-service broadcasting.

5   Managing critical Internet resources

74.   The ministers responsible for media and new communication services participating in the Reykjavik Conference in May 2009 adopted a *Resolution on Internet governance and critical Internet resources*[55] which recalls the obligation and commitment of member States to secure to everyone within their jurisdiction their fundamental rights and freedoms contained in the European Convention on Human Rights (ECHR). In this context, they underlined the importance of freedom of expression and information regardless of frontiers while at the same time stressing that access to the Internet is an important means by which large numbers of users are able to fully exercise and benefit from this right. They added that acts or events which block or significantly impede Internet access to or within fellow members of the international community may have significant implications under Article 10 of the ECHR, guaranteeing the right to freedom of expression and information.

75.   The Resolution refers to a shared responsibility by states to take reasonable measures through multilateral cooperation to ensure the ongoing functioning of the Internet and, in consequence, the delivery of the public service to which all persons under their jurisdiction are entitled. On this basis, the participating ministers called on all state and non-state actors to explore ways to ensure that critical Internet resources are managed in the public interest, and as a public asset, in full respect of international law, including human rights law. This could include, if appropriate, international supervision and accountability of the management of those resources.

76.   The Resolution also invites the CoE to explore the feasibility of developing a broad legal response to the need to protect the cross-border flow of media and media-like content and, more generally, Internet traffic having regard to Article 10 of the ECHR.

77.   In response to these proposals, it is expected that the competent intergovernmental cooperation body, the Steering Committee on the Media and New Communication Services (CDMC), be asked to give priority attention to the elaboration of legal instruments designed (i) to preserve or reinforce the protection of the cross-border flow of Internet traffic and (ii) to protect resources which are critical for the ongoing functioning and borderless nature and integrity of the Internet (i.e. critical internet resources). In this connection, the CDMC is expected to seek to ensure multi-stakeholder participation. An Ad-hoc Advisory Group on Cross-border Internet (MC-S-CI), made up of selected Internet governance experts, (including government, industry, civil society and academia) and reporting to the CDMC, has been asked to start considering these matters.

---

[55] http://www.coe.int/t/dghl/standardsetting/media/MCM(2009)011_en_final_web.pdf

6 Internet governance in the light of the WSIS principles

78.	As indicated in the introduction to this document, the multi-stakeholder and rights-based approach to Internet governance as reflected in the WSIS outcome documents and the IGF meetings since 2006 is supported by the CoE. This approach should be further reinforced in the future.

79.	The CoE has not only been contributing to the meetings of the IGF, but also supported the European Dialogue on Internet Governance (EuroDIG).[56] Following a first meeting at the CoE in Strasbourg in October 2008, a second meeting was held in Geneva at the European Broadcasting Union in September 2009 with some 250 participants. These meetings helped European actors interested in Internet governance discuss openly and freely their ideas, experiences and concerns in a fully multi-stakeholder format and prepare for the subsequent IGF events.

80.	In their Resolution *Internet governance and critical Internet resources*, the ministers responsible for media and new communication services participating in the Reykjavik Conference in May 2009 confirmed that pan-European efforts to enhance cooperation on Internet governance should have due regard to the CoE's values and standards on human rights, democracy and the rule of law, and the need for a multi-stakeholder approach. They acknowledged efforts to foster pan-European discussions on Internet governance bringing together state representatives and other stakeholders, such as the EuroDIG which is supported by the CoE. In conclusion, the ministers asked the CoE to make more lasting arrangements in this respect.

81.	Ministers declared that, in their standard-setting work, member States are inspired by the Tunis Agenda for the information society and the United Nations-led Internet Governance Forum (IGF).

82.	During its second edition, EuroDIG clearly emerged as the European IGF. Moreover, participants asked the CoE to provide it with the Secretariat. The Committee of Ministers - the governing body of the CoE - subsequently requested the Secretary General to make arrangements, in cooperation with relevant stakeholders and in partnership with European Union bodies, for the regular organisation of a European Dialogue on Internet Governance (EuroDIG) or pan-European Internet Governance Forum (IGF), with the CoE providing secretariat services.

83.	The Parliamentary Assembly of the CoE has underlined its appreciation of the useful work of the EuroDIG and the IGF. In paragraph 16.2 of its Recommendation 1882 (2009), the Assembly called on the CoE Committee of Ministers to "promote policies to make the Internet safer for children at the level of the European Dialogue on Internet Governance and the United Nations Internet Governance Forum and provide general support to the European Dialogue on Internet Governance, including secretariat support".[57]

84.	Moreover, the Council of Europe, the United Nations Economic Commission for Europe (UNECE) and the Association for Progressive Communications (APC) have been reviewing the arrangements for information and participation in entities concerned with Internet

---

[56] www.eurodig.org
[57] http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1882.htm

governance since the Rio de Janeiro meeting of the Internet Governance Forum in 2007. This has included an initial discussion paper, presented at an open workshop during the Hyderabad IGF in November 2008, and a second paper which mapped experience with information and participation in major Internet governance entities, which was discussed at an open meeting during the May 2009 IGF consultation in Geneva.

85.   The aim of the CoE/UNECE/APC project is to consider whether there is scope for developing a code of good practice on transparency, information and participation in Internet governance. Such a code could include principles and practical guidelines. It could build on existing Internet governance experience and the principles concerning Internet governance which were adopted at the WSIS, and could reflect and respond to growing interaction between the Internet and other spheres of public policy. In considering such a code of practice, existing practice in other public policy spheres, notably the UNECE Aarhus Convention which has introduced an inclusive approach to information, participation and transparency in environmental decision-making within the UNECE region, may be considered. A preliminary draft code will be presented for discussion at a workshop at the 2009 IGF.

7   Emerging issues: impact of social networks

86.   Many of the matters addressed in this paper apply *mutatis mutandis* to social networks, most particularly Sections 3.2 Protecting children's dignity, security and privacy on the Internet and 3.3 Protection of personal data and privacy, but also 4.2 Access for people with disabilities.

87.   Privacy issues must be resolved in order to ensure that social networks make a maximum contribution in terms of participation. Social networks are likely to develop in the near future as important tools for participation in a range of matters, not least in democratic processes. Activity in social networks may well influence considerably the outcomes of such processes. In addition to privacy (Article 8 of the European Convention on Human Rights), this concerns freedom of expression and information (Article 10) and the freedom of association (Article 11 of the European Convention on Human Rights).

88.   Moreover, the impact of social networks on children is of particular concern. The CoE Parliamentary Assembly's Rapporteur, Mr Jozsef Kozma, stated in his 2009 report on the promotion of Internet and online media services appropriate for minors: 58 "Social contacts and networks are expanding in the online world. Many of those are open to, and designed for, children and young people. The problem of adults grooming minors in online networks has been known for some years. Cyber bullying and harassment have been noted as a phenomenon more recently. With a growing part of the daily time spent on online networks, minors may also lose touch with real life and isolate themselves. The latter is sometimes referred to as cyber addiction." Following this report, the Parliamentary Assembly proposed in its Recommendation 1882 (2009) to analyse the potential psychological risks for children and adolescents using Internet and online media excessively, in particular social online networks suggesting virtual reality as well as violent online games and networks.59

---

58 http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc09/EDOC11924.htm

59 http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta09/EREC1882.htm

89. In this perspective, the "right to forget" also has great important. In the Declaration on protecting the dignity, security and privacy of children on the Internet, the CoE Committee of Ministers stated that, other than in the context of law enforcement, there should be no lasting or permanently accessible record of the content created by children on the Internet which challenges their dignity, security and privacy or otherwise renders them vulnerable now or at a later stage in their lives. It invited member States together, where appropriate, with other relevant stakeholders, to explore the feasibility of removing or deleting such content, including its traces (logs, records and processing), within a reasonably short period of time. This call has been reiterated by the Reykjavik Ministerial Conference.

The Council of Europe will be exploring these matters further.

8 Conclusions

90. The CoE will continue to support the multi-stakeholder and rights-based approach of the Internet Governance Forum. The IGF allows for open dialogue and the sharing of experience, and it can help promote the public service value of the Internet to ensure that it remains an open and accessible space.

91. The CoE is providing state and non-state actors with a range of almost ready-made tools, cooperation platforms, legal standards and public policy measures related to:

- the public service value of the Internet and a rights-based approach to Internet governance
- the freedom of expression and other fundamental rights in the online environment
- empowering children to make informed and safe use of ICTs
- the protection of children against abuse in connection with ICTs
- education and access to knowledge
- the protection of personal data and privacy
- the strengthening of security through measures against cybercrime, xenophobia and racism, the terrorist use of the Internet, and the counterfeiting of medicines and similar crimes that involve threats to public health.

92. Although developed in Europe, they may provide guidance to all stakeholders participating in the IGF, and countries outside Europe may want to consider accession to treaties such as the:

- Budapest Convention on Cybercrime (CETS 185)
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)
- Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data (CETS 108)
- Convention for the Prevention of Terrorism (CETS 196).

93. These and other tools to be developed by the CoE in the future should help the IGF advance security, openness and privacy, access and diversity, the management of critical Internet resources and the WSIS principles for Internet governance in view of creating opportunities for all.

_____