

***Committee of Experts on  
Rights of Internet Users  
(MSI-DUI)***



**3<sup>rd</sup> Meeting - 20 and 21 March 2013 (Strasbourg, Palais de l'Europe, Room 14)**

**Meeting report  
MSI-DUI (2013)05  
17 April 2013**

**Opening of the meeting and adoption of the agenda**

1. Gender distribution of the 29 attendants of the meeting: 9 women (32.03%) and 20 men (68.9%) (see Appendix 1).

2. The MSI-DUI adopted the agenda (Appendix 2) with the only change of postponing the election of the Chair and Vice-chair to the second day of the meeting.

3. Mr Jan Kleijssen, Director of the Information Society and Action against Crime Directorate, at the Directorate General of Human Rights and Rule of Law addressed the meeting. He acknowledged the good work carried out by the MSI-DUI and welcomed the participation of stakeholders in the meeting, in particular Facebook and the Internet Society.

4. Mr Kleijssen underlined that the focus of the Compendium must not be on new rights but on existing ones as foreseen and agreed by the Committee of Ministers. He also emphasised the importance of multi-stakeholder dialogue in the elaboration of the draft Compendium which includes stakeholder outreach, inclusion, partnership and transparency of processes. The European Dialogue on Internet Governance (EuroDIG) which will take place in Lisbon on 20 and 21 June and the Internet Governance Forum (Indonesia, 22-25 October) provide opportunities for this. The Conference of Council of Europe ministers responsible for media and information society (Belgrade, 7-8 November) will be another opportunity.

5. Mr Kleijssen referred to the EU's Charter of Passengers' Rights as an innovative way to raise awareness about people's rights and to improve their 'actionability'. Consequently, the type of document is one of the key questions to be addressed.

6. Mr Oluf Nielsen, DG-CONNECT, European Commission (EC), informed the MSI-DUI about the Code of EU Online Rights (the Code) which was released in December 2012. He gave an overview of the elements of the Code which related to the work of the MSI-DUI such as access to Internet content and services, the principle of minimum quality of service, personal data protection and the right to an effective remedy. He emphasised that the Code is not a legal instrument but a compilation of key digital rights which is usable only in EU member states.

## **Discussion and examination of draft Compendium of existing human rights for Internet users**

7. The Chair thanked all the MSI-DUI members for their contributions over a relatively short period of time between the Committee's meetings as well as the Secretariat for elaborating the first draft of the Compendium by consolidating members' inputs (Appendix 3). He stressed the need to resolve key questions, including the scope of the rights to be included in the Compendium, what should be the structure and order of included rights and the methodology of bringing together provisions of binding and non-binding standards. During discussions there was general consensus that the Compendium should employ easy to understand language for users.

8. The MSI-DUI members held an exchange of views on the content and form of the draft Compendium. Some members representing member states mentioned that they had had preliminary internal consultations and feedback in their capitals. Mr Alexander Borisov gave information about the positive feedback he had received, including the support of the Ministry of Foreign Affairs of the Russian Federation. He highlighted the balanced approach as regards rights and responsibilities.

9. Some members considered the draft to be, in parts, long and legalistic (freedom of expression, personal data protection) and that it could benefit from further elaboration in respect of the rights of children and the rights of people with disabilities. Greater attention to the positive obligations of member states was also highlighted as was the possible need to address issues of non-discrimination, participation in public affairs, aspects of the right to property and the need to operate in safe environments.

10. Mr Jan Malinowski, Head of Information Society Department, Directorate General of Human Rights and Rule of Law, stressed the need to respond to the terms of reference i.e. to produce a document to be endorsed by the Committee of Ministers based on consultation with stakeholders. He considered that the current version of the draft Compendium could be foreseen as part of a Committee of Ministers draft recommendation complete with an explanatory memorandum. Clear and concise wording for users, summarising key questions contained in captions or text boxes was considered as an innovative way to combine language destined for member states with the needs of a Compendium which addresses users.

### *Right to freedom of expression*

11. MSI-DUI members agreed that this chapter was quite advanced in comparison to others. Certain of its sections such as those on filtering and blocking should specify more clearly that they are concerned with interferences with this right. The safeguards provided for in Committee of Ministers recommendations should also contain a clearer indication of their source.

12. Some members considered that aspects of access to knowledge and culture would be better covered under the chapter on the right to education. Also, it was also suggested that the principle of anonymity be included in the draft Compendium, although some members, including the Chair, submitted questions regarding anonymity as a human right of Internet users. Formulations of sections on Internet access and access to information and services were also discussed and a number of wording suggestions were recorded during the meeting. MSI-DUI members had also a short exchange of views with the representative of Facebook with regard to processes that the company has put in place to address Internet users' complaints on alleged violations of their rights.

*Right to private and family life*

13. This chapter was considered as quite comprehensive although it would benefit from simpler formulations. Elements on tracking and profiling should be consolidated further. The differentiation between legally binding standards (Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (ETC No.108) and other standards, in particular Committee of Ministers recommendations (e.g. on search engines, and on social networking services) required attention. Default settings in social networking services should incorporate the highest levels of privacy protection.

*Right to freedom of assembly and association*

14. It was suggested to bring this chapter closer to the one on the right to freedom of expression. The parts covering effective remedies for this right as well as examples could be elaborated further. A new section on the right to online participation in public affairs was also mooted considering that the Internet is a catalyst for promoting democracy in different contexts.

*Online liberty and security*

15. Some MSI-DUI members submitted that there is a need to include aspects of unlawful intrusion in personal computers of Internet users such as identity theft, spam, phishing and botnets. It was agreed to consider this issue further on the basis of concrete Compendium language proposals by volunteering expert members. Combatting cybercrime is a common objective but reference to the Budapest Convention on Cybercrime should be tactful having regard to the views of different member states.

*Right to education*

16. It was agreed that this chapter be elaborated further including reference to access to knowledge, culture and media literacy.

*Freedom of thought, conscience and religion*

17. It was uncertain whether there should be a specific chapter on this or whether it can be adequately covered as part of the exercise of the right to freedom of expression. The debate resulted in a convergence of views that this freedom should provisionally stand on its own and its content should be elaborated further.

*Rights of the child*

18. Considering the extensive body of law on this matter, it was agreed that there should be a specific chapter on it. A specific chapter on the rights of people with disabilities was also agreed. The chapter could be framed in a more positive way by underlining the children's participation and empowerment, and their protection. Different age groups could be referred to in order to make the text more specific. Multi-stakeholder consultations should include children and young people.

### *Protection of property*

19. MSI-DUI members had an exchange of views on the desirability to have a new chapter on the right to property in relation to content or work produced by Internet users. It was agreed that volunteering members would provide concrete elements for this chapter, which should give a clear indication with regard the objective and the meaning of this part of the draft. The chair invited the MSI-DUI members to examine the draft Compendium with the objective of fulfilling the MSI-DUI mandate as adopted by the Committee of Ministers which focuses on existing rights.

### *Right to an effective remedy*

20. The issue of complementarity between the chapter on this right and the specific information on remedies included under each chapter and section was discussed. It was considered that for the time being it is useful to include as much information on specific remedies as possible under each section and to communicate clearly wherever it is considered that there is absence of remedies.

### **Multi-stakeholder outreach (interactions, consultations, participation in events)**

21. The MSI-DUI took note of the updated road-map of activities and had an exchange of views on the various rounds of multi-stakeholder consultation foreseen in it ([MSI-DUI\(2012\)09Rev](#)). Members expressed their interest and availability in participating in these activities and engaging with different stakeholders. The members who had attended the meeting of World Summit for Information Society +10 review (Paris, 25-27 February 2013) shared information on feedback received during a workshop organised by the Dynamic Coalition on Internet Rights and Principles 'Rights-Based Principles and the Internet: Taking Stock and Moving Forward' regarding the Council of Europe's initiative to develop the Compendium.

### **Election of Chair and Vice-chair**

22. Pursuant to [Resolution CM/Res \(2011\) 24](#) on intergovernmental committees and subordinate bodies, their terms of reference and working methods the MSI-DUI members re-elected Michael Kogler (Austria) as the Chairperson and Thomas Schneider (Switzerland) as the Vice-Chairperson for the period of time 14 September-31 December 2013.

### **Other business**

23. No other business was discussed.

### **Dates of next meeting**

24. The MSI-DUI members agreed to hold their fourth meeting on 1 and 2 October 2013 in Strasbourg. They also discussed the possibility of having an extra meeting in the course of 2013.

## **Appendix 1 List of Participants**

### **EXPERT MEMBERS**

Prof. Yaman AKDENIZ (Turkey / Turquie)  
Professor of Law, Faculty of Law, and Pro-Rector for the Istanbul Bilgi University -

Prof. Dr. Wolfgang BENEDEK (Austria / Autriche)  
Institute for International Law and International Relations, University of Graz

Mr Alexander BORISOV (Russian Federation / Fédération de Russie)  
Professor, Moscow State Institute of International Relations

Mr Hasan Ali ERDEM (Turkey / Turquie)  
Expert, International Relations Department, Turkish Radio and Television Supreme Council (RTÜK)

Mr Johan HALLENBORG (Sweden / Suède)  
Deputy Director, Department for International Law, Human Rights and Treaty Law, Ministry for Foreign Affairs

Ms Dixie HAWTIN (United Kingdom / Royaume-Uni)  
Project Manager, Freedom of Expression, Global Partners & Associates

Ms Rikke Frank JORGENSEN (Denmark / Danemark)  
Special Adviser, The Danish Institute for Human Rights

Dr Michael KOGLER, Chairperson (Austria / Autriche) (**CHAIR**)  
Deputy Head of Department for Media Law, Constitutional Service, Federal Chancellery

Ms Eva KUSHOVA (Albania / Albanie)  
Press Adviser, Ministry of Foreign Affairs

Ms Meryem MARZOUKI (France)  
EDRi & CNRS / Université Pierre et Marie Curie (Paris VI)

Mr Thomas SCHNEIDER (Switzerland / Suisse)  
Deputy Head of International Relations Service, Coordinator international Information Society, International Affairs, Federation Office of Communication, Federal Department for the environment, transport, energy and communication

Ms Nelly STOYANOVA (Bulgaria / Bulgarie)  
National expert, Body of European Regulators for Electronic Communications (BEREC)

Mr Francisco TEIXEIRA da MOTA (Portugal)  
Lawyer, Freedom of expression and media

## **PERMANENT REPRESENTATIVES OF THE COUNCIL OF EUROPE**

Mr Matthew JOHNSON, Ambassador Extraordinary and Plenipotentiary, Permanent Representative of the United Kingdom to the Council of Europe - *Apologised*

## **PARTICIPANTS DESIGNATED BY MEMBER STATES**

Mr Tanel TANG, Deputy to the Permanent Representative, Permanent Representation of Estonia to the Council of Europe

Mr Mustafa ÖZDEMİR, Information Expert, Information and Communications Technologies Authority of the Republic of Turkey (ICTA), Ankara

## **PARTICIPANTS**

### **European Audio-visual Observatory / Council of Europe**

Ms Susanne NIKOLTCHEV, Head of Department for Legal Information - *Apologised*

### **European Commission**

Mr Oluf NIELSEN, European Commission, D1 International, CONNECT Directorate General, European Commission

### **Organisation for Security and Cooperation in Europe (OSCE)**

Mr Roland BLESS, Principal Adviser, Representative on Freedom of the Media - *Apologised / Excusée*

### **UNESCO**

Ms Xianhong HU, UNESCO, Division for Freedom of Expression, Democracy and Peace - Communication and Information Sector - *Apologised*

## **INVITED STAKEHOLDERS**

### **Article 19**

Ms Gabrielle GUILLEMIN, ARTICLE 19, London, United Kingdom -- *Apologised*

### **ENPA**

Mr Holger ROSENDAL, Member of the European Newspaper Publishers' Association (ENPA), Chefjurist at the Danish Newspaper Publishers' Association (*Danske Dagblades Forening - DDF*) Copenhagen, Denmark - *Apologised*

### **EuroISPA**

Mr Michael ROTERT, Honorary Spokesman

### **European Youth Forum (EYF)**

Ms Triin ADAMSON (title to be confirmed)

### **Facebook**

Ms Melina VIOLARI, Policy & Privacy Manager, Brussels, Belgium

### **Global Network Initiative**

Mr David SULLIVAN, Policy and Communications Director - *Apologised*

**Google**

Mr Marco PANCINI, Senior Policy Counsel - *Apologised*  
Ms Dorothy CHOU, Public Policy - *Apologised*

**International Chamber of Commerce**

Mr Thomas SPILLER, Walt Disney Company - *Apologised*

**Twitter International Company**

Ms Sinéad McSWEENEY, Director of Public Policy/EMEA - *Apologised*

**YAHOO!**

Mr Patrick ROBINSON, Director, Business and Human Rights - *Apologised*

**Internet Society (ISOC)**

Mr Nicolas SEIDLER

**COUNCIL OF EUROPE SECRETARIAT**

Mr Jan KLEIJSEN, Director, Information Society and Action against Crime Directorate,  
Directorate General of Human Rights and Rule of Law

Mr Jan MALINOWSKI, Head of Information Society Department, Directorate General of  
Human Rights and Rule of Law

Mr Lee HIBBARD, Head of Internet Governance Unit, Directorate General of Human  
Rights and Rule of Law

Ms Elvana THAÇI, Administrator, Internet Governance Unit, Directorate General of Human  
Rights and Rule of Law

Mr Pawel MAKOWSKI, Study visitor, Data Protection Unit

Mr Philippe KRANTZ, Secretariat of the European Committee on Legal Co-operation  
(CDCJ) - *Apologised*

Mr Rüdiger DOSSOW, the Committee on Culture, Science, Education and Media,  
Parliamentary Assembly of the Council of Europe

Ms Stéphanie BUREL, Lanzarote Committee, Children's Rights Division, Directorate  
General of Human Rights and Rule of Law

Mr Rui GOMES / Mr Laszlo FÖLDI, Education and Training, Youth Department,  
Directorate for Democratic Participation and Citizenship

Mr Matthias KLOTH, Administrator, Human Rights Law and Policy Division, Directorate  
General of Human Rights and Rule of Law - - *Apologised*

Ms Bogumila WARCHALEWSKA-MULLER, Directorate of Policy Planning

Ms Sonya FOLCA, Assistant, Internet Governance Unit, Directorate General of Human  
Rights and Rule of Law

## **Appendix 2 Annotated Agenda**

### **1. Opening of the meeting**

### **2. Adoption of the agenda**

The members of the MSI-DUI are invited to adopt the agenda of the meeting.

### **3. Election of Chair and Vice-Chair**

The members of the MSI-DUI are invited to elect the Chair and the Vice-Chair pursuant to article 12 of the Rules of procedure for Council of Europe intergovernmental committees.

*Reference document:* [Resolution CM/Res \(2011\) 24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods](#)

### **4. Information of relevance to the work of the MSI-DUI by the Secretariat**

The Secretariat will provide updated information to the MSI-DUI on the Council of Europe activities relating to corporate social responsibility in the field of human rights, proposals on the modernisation of Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (ETC No.108) and the relevant activities of the Parliamentary Assembly of the Council of Europe (PACE).

*Reference documents:* Decision of the Deputies at the 1160th meeting (30 January 2013) [CM/Del/Dec\(2013\)1160/4.1](#).

Modernisation Proposals adopted by the 29<sup>th</sup> plenary meeting of the Consultative Committee of the Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (ETC No.108) [T-PD\(2012\)4Rev3\\_en](#) .

Background report for the PACE Committee on Culture, Science, Education and Media: The Right to Internet Access - Rapporteur: Ms. Jaana PELKONEN, Finland (EPP/CD), AS/Cult (2013) 08

[Code of EU online Rights](#)

### **5. Discussion and examination of draft Compendium of existing human rights for Internet users**

The MSI-DUI members are invited to discuss, examine and update the draft Compendium.

*Reference and working documents:* Draft Compendium of existing human rights for Internet Users (MSI-DUI(2013)03)



[MSI-DUI Terms of Reference](#)

*Report of the 2<sup>nd</sup> meeting of the MSI-DUI (MSI-DUI(2013)02)*

*Discussion paper mapping-out issues regarding a Compendium of Rights of Internet Users –by Wolfgang Benedek, University of Graz/UNI-ETC ([MSI-DUI\(2012\)03](#))*

**6. Multi-stakeholder outreach (interactions, consultations, participation in events)**

The members of the MSI-DUI will be invited to debrief on the activities or events in which they have participated and that are of interest to the work of the Committee. They will be invited to assess progress in multi-stakeholder outreach and to prepare for next steps in with the agreed road-map, notably the European Dialogue on Internet Governance (20-21 June 2013, Lisbon) and the Internet Governance Forum (TBC).

Working document: Roadmap for multi-stakeholder consultations (MSI-DUI(2012)09Rev)

**7. Other business**

Issues not covered by other items of the agenda should be discussed.

**8. Dates of next meeting**

The MSI-DUI members will be invited to agree on the dates of its next meeting in 2013.

**Appendix 3**  
**Draft Compendium of existing human rights for internet users\***

**7 March 2013**

<b>Introduction.....</b>	<b>11</b>
<b>FREEDOM OF EXPRESSION.....</b>	<b>11</b>
Internet access .....	12
Access to information (content & services) .....	13
Freedom from blocking and filtering .....	14
Content removal and account deactivation .....	16
Access to knowledge and culture.....	17
<b>RIGHT TO RESPECT FOR PRIVATE LIFE.....</b>	<b>18</b>
Personal data protection .....	18
Principles and standards on the use of personal data .....	19
Freedom from interception and monitoring/surveillance .....	20
Tracking.....	21
Profiling.....	22
<b>ONLINE LIBERTY AND SECURITY.....</b>	<b>23</b>
<b>RIGHT TO ONLINE ASSEMBLY AND ASSOCIATION.....</b>	<b>23</b>
<b>FREEDOM OF RELIGION.....</b>	<b>24</b>
<b>RIGHT TO EDUCATION.....</b>	<b>24</b>
<b>RIGHTS OF PEOPLE WITH DISABILITIES .....</b>	<b>24</b>
<b>RIGHTS OF THE CHILD .....</b>	<b>25</b>
<b>PROTECTION OF PROPERTY .....</b>	<b>26</b>
<b>RIGHT TO AN EFFECTIVE REMEDY .....</b>	<b>26</b>

---

\* The page numbers of chapter appearing in the table of contents corresponds to the page numbering of the draft Compendium as included in the document prepared by the MSI-DUI.

## Introduction

---

The Internet creates new opportunities for people's access to information, their social, political and everyday activities. At the same time the Internet brings new challenges for the full enjoyment and exercise of fundamental rights and freedoms. Human rights must be protected equally offline and online.

The Compendium aims at raising users' awareness of their human rights and fundamental freedoms on the Internet by providing guidance to them on the application of existing standards in Internet and online environments. The objective is to help users understand and exercise their rights when they communicate with and seek effective recourse from key Internet actors and government agencies.

The Compendium does not foresee new rights and freedoms but only those that are already provided for in existing international instruments, notably in the European Convention on Human Rights (ECHR). It offers interpretation and explanations of their application online. Its focus is on particular rights and freedoms which are considered as mostly affected by the Internet. The Compendium does not have a legal status (it is not enforceable) and it is without prejudice to the enforceability of the legal instruments on the basis of which it is elaborated.

## **FREEDOM OF EXPRESSION**

[*Right*] Everyone has the right to freely express his/her opinion, views, ideas and to receive and impart information via the Internet regardless of frontiers.

[*Restriction*] Freedom is not unlimited – rights may be subject to formalities, conditions, restrictions or penalties. There are three conditions for admissible limits:

- must be prescribed by law;
- must pursue a legitimate aim;
- must be necessary in a democratic society.<sup>1</sup>

[*Remedies*] Appeal to a competent authority (ombudsperson) and/or judicial authority.

### *[Examples/explanations]*

Interferences with the right to freedom of expression must be provided by a strict legal framework regulating the scope of the restrictions which is accessible, clear and precise as to enable everyone concerned to regulate his/her behaviour in the field and effective as to the judicial control in order to prevent abuse.<sup>2</sup>

Interferences must pursue a legitimate aim in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. The list of the possible grounds for restricting the freedom of expression exhaustive.

---

<sup>1</sup>Some MSI-DUI members suggest to replace this section with a restatement of Article 10 of the ECHR.

<sup>2</sup>Yildirim v. Turkey, (no 3111/10), the ruling is not final yet.

Interferences must be necessary in a democratic society – corresponding to a pressing social need, proportional to the legitimate aim pursued, the least restrictive means for achieving it<sup>3</sup> and justified by judicial decisions that are relevant and sufficient in reasoning.<sup>4</sup>

On matters of general interest<sup>5</sup> there is a higher level of protection for the right to freedom of expression in the area of political, militant and polemical expression and debate. Freedom of expression extends also to information or ideas that offend shock or disturb the State or any section of the population.<sup>6</sup>

The expression of views and opinions that are directed against the values of the ECHR, for example but not limited to anti –semitic or islamophobic remarks do not benefit from freedom of expression guarantees. Measures taken to restrict hate speech<sup>7</sup>, discrimination, intolerance and glorification of terrorism can be regarded as answering a pressing social need if all three conditions as mentioned above (as interpreted by the European Court of Human Rights (ECtHR)) are met.<sup>8</sup>

Restrictions on the right to freedom of expression may be justified in the context of protecting children from physical and moral risks such as child pornography<sup>9</sup> and young people from accessing obscene pictures<sup>10</sup>.

Restrictions on the expression of views which amount to defamation could be found as justifiable in order to protect the reputation and rights of others where all the conditions mentioned above are met.<sup>11</sup>

### Internet access

*[Right]* Everyone should be enabled to access a minimum set of Internet services at an affordable price and irrespective of age, gender, race, religion, political or other opinion, national, ethnic or social origin, association with a national minority property, birth or other status. This also applies to individuals living in rural and geographically remote areas, those with low incomes and those with special needs (for example disabled persons).<sup>12</sup>

*[Restriction]* Any restriction imposed on Internet accessibility, such as complete discontinuation or limitations of Internet access by the state or a private entity interferes

---

<sup>3</sup> Ibid, the Court's opinion asserts that measures rendering a big quantity of information inaccessible affect considerably the rights of Internet users and have an important collateral effect. Obligation of domestic judges to examine the necessity of a total blockage of a site, see para.61, 66, 67 of the opinion.

<sup>4</sup> Zana v. Turkey (69/1996/688/880); Fressoz and Roire v. France (no. 29183/95); Surek v Turkey (no. 26682/95).

<sup>5</sup> Willem v. France (no. 10883/05); Feret v. Belgium (no 15615/07); Renaud v. France (no 13290/07).

<sup>6</sup> Handyside v. UK (no. 5493/72); Perrin v. UK (no. 5446/03).

<sup>7</sup> [Recommendation No. R 97 \(20\)](#) of the Committee of Ministers of the Council of Europe on "hate speech" states that "hate speech" is understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.

<sup>8</sup> Surek v. Turkey (no. 26682/95); Gunduz v. Turkey (no. 35071/97); Feret v. Belgium (no 15615/07);

<sup>9</sup> K.U. v Finland (no. 2872/02)

<sup>10</sup> Perrin v. UK (no. 5446/03).

<sup>11</sup> Bargao et Domingos Correia v. Portugal (nos 53579/09 et 53582/09); Perrin v. UK (no. 5446/03); Lindon, Otchakovsky-Laurens and July v. France (nos 21279/02 36448/02).

<sup>12</sup> ECHR, Art.10; Art 14; Art. 1 protocol 12; Recommendation [CM/Rec\(2007\)16](#) of the Committee of Ministers to member states on measures to promote the public service value of the Internet, section II; [Recommendation No. R \(99\)14 of the Committee of Ministers](#) to member states on universal community service concerning new communication and information services, principle 1;

with the right to receive and impart information.<sup>13</sup> Such restrictions can only be accepted if they meet the conditions Article 10 para.2.

*[Safeguards]* Before an Internet disconnection measure is taken, Internet users should receive notice/information regarding the legal basis, the grounds and the procedures for objecting such measures. They should be offered the means to request a reinstatement of full access to the Internet. Such requests should be treated within reasonable time limits.

*[Remedy]* Every Internet user has the right to have any Internet connection measure reviewed by competent administrative and judicial authorities.

*[Examples]* In some countries, laws are being passed which allow for an individual's internet access to be cut entirely following violation of intellectual property rights law. Such laws are disproportionate regardless of the process followed and therefore a violation of freedom of expression.<sup>14</sup>

In some countries measures are being introduced which limit access to the Internet, such as imposing registration or other requirements on service providers. These measures will not be legitimate unless they conform to the tests for restrictions on freedom of expression. Internet Service Providers may cut an individual's Internet access because that individual has not paid for the service. This may be legitimate however, the company should introduce policies and measures which prevent violation of the right to freedom of expression and which provide remedies in the event that a violation occurs.

### Access to information (content & services)

#### *[Policy principles and safeguards]*

- (1) Every Internet user should have the greatest possible access to Internet-based content, applications and services of his/her choice, whether or not they are offered free of charge, using suitable devices of his/her choice. Such a general principle, commonly referred to as network neutrality, should apply irrespective of the infrastructure or the network used for Internet connectivity.<sup>15</sup>
- (2) Users should be adequately informed about any network management measures that affect in a significant way access to content, applications or services. In particular, these measures should be proportionate, appropriate and avoid unjustified discrimination; they should be subject to periodic review and not be maintained longer than strictly necessary.<sup>16</sup>
- (3) Every Internet user is entitled to have transparent information in respect of selection and hierarchical ordering of the information they receive, in particular as

<sup>13</sup> Autronic AG v Switzerland (No. 12726/87); Yildirim v. Turkey (no 3111/10).

<sup>14</sup> The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue has stated in his report A/HRC/17/27 "The Special Rapporteur considers cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights.". See paragraph 74, available at [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf)

<sup>15</sup> [Declaration of the Committee of Ministers on Network Neutrality](#), adopted by the Committee of Ministers on 29 September 2010; Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, article 8(4) g;

<sup>16</sup> [Declaration of the Committee of Ministers on Network Neutrality](#).

regards the criteria according to which information is selected, ranked and prioritised (for example in search results);<sup>17</sup>

[*Remedies*] There should be adequate avenues respectful of rule of law requirements, to challenge network management decisions and, where appropriate, there should be adequate avenues to seek redress.<sup>18</sup>

[*Examples*] Network operators may engage in network management practices which may block or prioritise certain types of content and applications over others. For example, certain operators may block peer-to-peer protocols, slow down traffic carrying video or webcasting or charge for such traffic. These practices affect Internet users' ability to have access to Internet content and services.

### **Freedom from blocking and filtering**

[*Right*] The Internet user has a right not to be denied access to legal content on the Internet by filtering and blocking measures carried out by the state or by non-state actors such as Internet Service Providers.

#### ***[Policy principles]***

- (1) Any restriction on access to Internet content may constitute a violation of freedom of expression and the right to receive and impart information if the conditions of Article 10(2) of the ECHR are not met.<sup>19</sup> Measures which result in blocking access to and filtering Internet content are not a priori incompatible with the ECHR. However, they should be prescribed by a strict legal framework to regulate the scope of the ban and affording the guarantee of judicial review to prevent possible abuses.<sup>20</sup>
- (2) Public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers. Nationwide general blocking or filtering measures by state authorities can only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body in accordance with the requirements of Article 6 of the ECHR.<sup>21</sup> A measure aimed at blocking specific Internet content must not be used as a means of general blocking.<sup>22</sup>
- (3) These requirements do not prevent the installation of filters for the protection of minors in specific places where minors access the internet such as schools or libraries.<sup>23</sup> Filters in schools and libraries should not restrict the right to receive and impart information of non-minors.

---

<sup>17</sup> Recommendation [CM/Rec\(2012\)3](#) of the Committee of Ministers to member States on the protection of human rights with regard to search engines

<sup>18</sup> See note 15 above.

<sup>19</sup> Recommendation [CM/Rec\(2008\)6](#) of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters.

<sup>20</sup> *Yildirim v. Turkey* (no 3111/10).

<sup>21</sup> See note 19 above.

<sup>22</sup> *Yildirim v. Turkey* (no 3111/10).

<sup>23</sup> Committee of Ministers [Declaration on Freedom of Communication on the Internet](#).

- (4) General blocking and filtering of Internet content by Internet intermediaries such as the blocking by search engines of all search results for certain keywords should meet the requirements of Article 10. Internet content that has been determined by a competent authority as harmful for certain categories of Internet users should not be subjected to general de-indexation for all categories of Internet users.<sup>24</sup>

*[Rights and safeguards]* Internet users are entitled to:

- (i) information that enables them to identify when filtering has been activated and to understand how, and according to which criteria, the filtering operates;
- (ii) information about de-indexation or filtering of specific websites or content by search engines;<sup>25</sup>
- (iii) information that enables them to understand why a specific type of content has been filtered;
- (iv) concise information and guidance regarding the manual overriding of an active filter, namely who to contact when it appears that content has been unreasonably blocked and the reasons which may allow a filter to be overridden for a specific type of content or URL;
- (v) effective and readily accessible means of recourse and remedy, including suspension of filters, in cases where users claim that content has been blocked unreasonably.

*[Remedy]* The Internet service providers should implement readily accessible means of communication for users and/or authors of content to report on unreasonable blocking of content and to appeal against decisions on blocking and filtering.

The state must provide for effective and readily accessible means of recourse in cases where users and/or authors of content claim that content has been blocked unreasonably. If content is found to be blocked unreasonably, the state must provide for remedy, including suspension of filters. As a last recourse the user shall be afforded easy access to raise a complaint with the national courts, and if national remedies is exhausted, to the ECtHR.

*[Example]* Internet users should receive the necessary information to make them aware about blocking and filtering measures such as black lists, white lists, keyword blocking, content rating, de-indexing of content by search engines, other means as well as combinations of these.

Sometimes Internet users are provided with a simple error message such as 'File not found' or 'Forbidden' when they request to access certain content which has been blocked or filtered. Such information may not be sufficient to enable the affected of instances in which the filters operate to block access to a particular website in order to be able to challenge the decision to filter or block.

---

<sup>24</sup> See note 17 above.

<sup>25</sup> Ibid.

### **Content removal and account deactivation**

#### *[Policy principles]*

- (1) Removal of user-created content by Internet-based platforms that host such content as well as deactivation of a user's account may violate the right to freedom of expression and the right to receive and impart information and as such must fulfil the conditions of Article 10(2) of the ECHR<sup>26</sup>.
- (2) Internet-based platforms that host user-created content may exercise different levels of editorial control in accordance with rules explicitly stated in their policies or in the terms and conditions. Internet-based platforms should ensure that the right to freedom of expression is guaranteed in compliance with Article 10 of the ECHR.<sup>27</sup> They should refrain from conveying hate speech and other content that incites violence or discrimination for whatever reason. Special attention is needed on the part of actors operating collective online shared spaces which are designed to facilitate interactive mass communication. They should be attentive to the use of, and editorial response to, expressions motivated by racist, xenophobic, anti-Semitic, misogynist, sexist (including as regards LGBT people) or other bias.<sup>28</sup>

#### *[Right]*

- (1) Where Internet platforms intend to take measures to remove user-generated content or deactivate a user's account the concerned Internet user should be informed and be given the possibility to respond to the situation on a volunteer basis.
- (2) In the case of removal of content created by a user or deactivation of his/her account, he/she should be enabled to have accessible (in a language that understands) clear and precise information regarding the fact of and the grounds for such actions as well as an explanation as to whether it is prescribed by law, pursues a legitimate aim and is proportional to the legitimate aim pursued.
- (3) Every Internet user should be enabled to appeal decisions on content removal and account de-activation with the Internet service/online provider. The appeal process should be in compliance with due process requirements (the Internet user should receive information about the grounds for removal or de-activation, about the duration of the appeal process; the appeal should be processed in a reasonable time; the user should be given all the necessary explanations why the content was removed or account deactivated, and if the appeal is denied the reasons why it was denied).
- (4) Every Internet user should be enabled to appeal the decision of the Internet service/online provider with a competent administrative judicial authority.

---

<sup>26</sup> Recommendation [CM/Rec \(2011\)7](#) of the Committee of Ministers to member states on a new notion of media, paras.68, 69 ; Recommendation [CM/Rec\(2012\)4](#) of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, para 3

<sup>27</sup> [CM/Rec \(2011\)7](#), paras.18; 30-31

<sup>28</sup> [CM/Rec \(2011\)7](#), para 91.



- (5) Every Internet user should be enabled to signal and report to the hosting platform through easily accessible mechanisms the existence of content or expression of views and/or behaviour that are apparently illegal content or behaviour.<sup>29</sup>

*[Remedy]*

Appeal to the Internet platform. Appeal to competent institutions (e.g. ombuds-person) judicial remedy.

*[Example]*

User-generated content platforms (Twitter, Facebook, others) generally establish in their Terms of Use or other policies which types of content and behaviours they consider as inappropriate as well as procedures for content removal and account deactivation when they consider that their Terms of Use are violated. They also adopt tools and processes for identifying and reporting violations of their Terms of Use such as user-driven flagging mechanisms, automated responses based on pre-determined criteria, community or peer review, which vary depending on the form of content or activity allowed in the platform.

When a violation of Terms of Use is detected or reported the concerned platform should convey warnings or notices (email notice, pop-up window) of violations to users which should be transparent and timely, describing the specific rules allegedly violated, providing links to information explaining the provider's process for responding to users' communications and clearly explaining the next steps for appeal.

Different platforms offer different tools for reporting inappropriate content or behaviour, e.g. Facebook: Report/block this person.

**Access to knowledge and culture**

*[Right]* In the exercise of their right to freedom of expression Internet users should be enabled to access digital education, cultural, scientific, scholarly and other content in their languages and in relation to their cultures so as to ensure that all cultures can express themselves and have access to the Internet in all languages.<sup>30</sup> The Internet user shall be able to freely access publicly funded research and cultural works on the Internet. Access to digital heritage materials should be ensured within reasonable restrictions.<sup>31</sup> Internet users should have the possibility to create, modify and remix interactive content.<sup>32</sup>

*[Restrictions]* Restrictions on access to knowledge are permitted in specific cases in order to remunerate authors for their work. Remuneration of authors shall be carried out in ways which allow for further innovation and access to public and educational knowledge and resources.

*[Remedies]* The state must provide for effective and readily accessible means of recourse in cases where users claim that their access to knowledge on the internet is unreasonably restricted. If content is found to be restricted unreasonably, the state must provide for remedy, if at all possible. As a last recourse the user shall be afforded easy access to raise a complaint with the national courts, and if national remedies is exhausted, to the ECtHR.

---

<sup>29</sup> Ibid., para 91; [CM/Rec\(2012\)4](#), II/10.

<sup>30</sup> See note 12 above, [CM/Rec\(2007\)16](#) Section IV.

<sup>31</sup> Ibid.

<sup>32</sup> Ibid.

[Example] to be completed.

### **RIGHT TO RESPECT FOR PRIVATE LIFE**

According to Article 8 of the ECHR:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

The right to private life includes the right to identity and personal development, the right to establish and develop relationships with other human beings and the outside world and may include activities of a professional or business nature. Private life is a broad notion not susceptible to exhaustive definition.<sup>33</sup>

### **Personal data protection**

[Right] Everyone has the right to privacy with regard to personal data on the Internet.

Everyone whose personal data are processed by any public authority, company or individual (data controller) on the Internet:

- (1) should be informed when his/her personal data is processed and about the data controller's identity and habitual residence or principal place of business;
- (2) is entitled to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him/her is stored as well as communication to him/her of such data in an intelligible form;
- (3) is entitled to obtain rectification or erasure of such data if these have been processed contrary to the law giving effect to basic principles of personal data processing;
- (4) is entitled to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to above is not complied with.<sup>34</sup>

[Restriction] Data processing by public authorities and private entities amounts to an interference with the right to privacy with regard to personal data.<sup>35</sup> Derogations from the right to privacy with regard to personal data shall be allowed only when the conditions of Article 8, paragraph 2 are met. Restrictions of the rights foreseen in paragraphs 1, 2 and 3 may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.<sup>36</sup>

[Remedy] Everyone has the right to appeal to competent authorities (for example data protection authorities) if the rights above are not respected.

<sup>33</sup> Rotaru v Romania (no. 28341/95); P.G. and J.H. v the UK (no. 44787/98); Peck v. UK (no. 44647/98); Perry v. UK (no. 63737/00); Amann v. Switzerland (no. 27798/95).

<sup>34</sup> Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (ETC No.108, art. 8.

<sup>35</sup> Leander v Sweden (no. 9248/81), para 48.

<sup>36</sup> See note 34, art. 9.

*[Example]*

Internet users increasingly search for information on the Internet with the help of search engines. These process large amounts of personal data based on the search behaviour histories of individuals which may reveal the person's beliefs, relations or intentions, sensitive data revealing racial origin, political opinions, religious or other beliefs, data concerning health, sexual life or relating to criminal convictions. Search engines should ensure full respect for the data processing principles of data minimisation, retention periods, and protection against unlawful access by third parties. They should be in a position to provide easily accessible information to users about the reasons for collection and retention of their personal data and intended uses thereof. They should also inform individuals about the exercise of their rights in an intelligible form, using clear and plain language adapted to the data subject. Cross-correlation of data originating from different services/platforms belonging to the search engine provider should be performed only if unambiguous consent has been granted by the user for that specific service.<sup>37</sup>

Internet users also share large amounts of personal information and data on social networks. In order to be able to exercise their right to privacy they should have access and use default settings to limit access to personal information by the public at large and/or specific individuals or parties. They should be given adequate tools to give their informed consent to any type of processing of any specific type of personal data, including those contained in audio and video content, which permits access by third parties and to withdraw such consent and to remove personal data stored about them, delete their profiles and permanently eliminate data from storage. Internet users should also have information about the applicable law and jurisdiction in relation to the processing of their personal data.<sup>38</sup>

**Principles and standards on the use of personal data**

(1) The compiling and storing of personal data, the carrying out logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination must meet the following privacy protection standards, personal data must be:

- obtained and processed fairly and lawfully;
- stored for specified and legitimate purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are stored;
- accurate and, where necessary, kept up to date;
- preserved in a way which permits identification of the data subject for no longer than is required for the purpose for which those data are stored;<sup>39</sup>

(2) Sensitive data – personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life – may not be processed automatically unless the law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.<sup>40</sup>

---

<sup>37</sup> See note 17 above.

<sup>38</sup> See note 26 above.

<sup>39</sup> See note 34 above, art.5

<sup>40</sup> Ibid, art. 6.

(3) Security of data – appropriate security measures should be taken to ensure the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.<sup>41</sup>

### Freedom from interception and monitoring/surveillance

*[Right]* Everyone has the right to respect for the confidentiality of his/her correspondence and communications such as email, messages, instant messaging or other forms of communications via/on the Internet.

*[Restriction]* Interferences with this right can only be accepted if they are in compliance with the conditions of Article 8 para. 2 of the ECHR.

*[Remedy]* Any individual who has been subject to such measures has the right to appeal to competent judicial authorities

*[Explanations]* The ECtHR has developed general principles with particular reference to the requirements that the law which provides for interception of correspondence and communications by public authorities should meet. The law must be accessible by everyone concerned, clear and precise to give citizens an adequate indication of the conditions and circumstances in which authorities are empowered to resort to such measure, in particular with regard to

- (i) the nature of the offences which may give rise to an interception order;
- (ii) the definition of the categories of people liable to have their communications monitored;
- (iii) the limit on the duration of such monitoring;
- (iv) the procedure to be followed for examining, using and storing the data obtained; and
- (iv) the precautions to be taken when communicating the data to other parties; and the circumstances in which data obtained may or must be erased or the records destroyed<sup>42</sup>.

Also, measures taken by public authorities which consist of observing and monitoring the actions of an individual, the systematic recording and storing of information relating to an individual Internet user's private life as well as the use and disclosure of information obtained [and the refusal to allow an opportunity for such information to be refuted] constitute interferences with the right to private life.<sup>43</sup>

The ECtHR has developed general principles with particular reference to the requirements that the law which provides for monitoring should meet. The law must be accessible by every person concerned and sufficiently precise and clear to give citizens an adequate indication of the conditions and circumstances in which authorities are empowered to resort to such measures, in particular with regard to (i) the nature of the measure (technical means used); (ii) the scope of the measure (the kind of information that may be

<sup>41</sup> See note 34 above. art 7.

<sup>42</sup> Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria (no. 62540/00)

<sup>43</sup> Rotaru v Romania (no. 28341/95); P.G. and J.H. v the UK (no. 44787/98); Peck v. UK (no. 44647/98); Perry v. UK (no. 63737/00); Amann v. Switzerland (no. 27798/95); Weber and Saravia v Germany (no. 54934/00); Liberty and others v. the UK (no. 58243/00); Klass and others v. UK (no. 5029/71); Uzun v Germany (no. 35623/05).

gathered and kept and the categories of people against whom surveillance measures can be taken);(iii) the length of time for which the information may be kept and the time limitation for the duration of surveillance measures in proportion with the circumstances;(iv) the grounds required for authorising surveillance ( the circumstances in which such measures may be taken);(v) the authorities competent to permit, carry out and supervise the surveillance measures;(vi) the kind of remedy provided by law (effective supervision by a judicial authority (at least in the last resort, as it affords the best guarantees of independent, impartial control according to a proper procedure.)<sup>44</sup>

### Tracking

[*Right*] In the case of storing of information, or gaining of access to information already stored in the terminal equipment of an Internet user, he/she is entitled to:

- (1) clear and comprehensive information about the purposes of the storage of, or access to, that information processing of personal information;
- (2) give his/her consent to such storing of information or access to stored information.

[*Restriction*] Informed consent will not apply to technical storage of, or access to, information

- (1) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
- (2) where such storage or access is strictly necessary in order for the provider of an information society service requested by the Internet user.<sup>45</sup>

[*Remedy*] Appeal to online service providers, appeal to data protection authorities or other competent authority, judicial remedies.

### [Example]

Personal data of an Internet user may be collected and processed in the context of his/her interaction with a website or an application or in the context of Internet browsing activity over time and across different websites e.g. pages and content visited, times of visits, what was searched for, what was clicked (tracking). Cookies are one of the technologies/techniques used to track users' browsing/online activities by storing information in a user's equipment and retrieving it.

Internet users can exercise/signify their right to consent by setting, amending, managing controls on the Internet browsers that they use - e.g. using options to delete, block or disable cookies in web browsers that offer these capabilities. Various web browsers (Microsoft, Mozilla, Chrome) offer do-not-track capabilities.

---

<sup>44</sup> Id.

<sup>45</sup> Directive 2009/136/EC, article 5/3: "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

Profiling<sup>46</sup>

[Right] In the case of profiling, understood as automatic data processing techniques which consist of applying a profile to an individual in order to take decisions concerning him or her or for analysing or predicting his or her personal preferences, behaviours and attitudes – the Internet user to whom profiling is applied is entitled to:

- receive information that his/her personal data will be used in the context of profiling, the purpose of profiling, categories of personal data used, the identity of the controller;
- obtain from the controller at his/her request, within a reasonable time and in an understandable form information concerning his/her personal data, the logic underpinning that was used to attribute a profile to him/her, the purposes of profiling and categories to whom the data may be communicated;
- freely give his/her informed and specific consent to profiling and to withdraw consent;
- secure correction, deletion or blocking of their personal data where profiling is carried out contrary to the principles of law;
- object the use of his/her personal data for profiling;
- receive information where there are grounds for restricting the above-mentioned rights and information how to challenge this before a competent national supervisory authority or a court;
- object a decision having legal effects concerning him/her or significantly affecting him/her taken on the sole basis of profiling unless this is provided by law enabling him/her to put forward his point of view.

[Restriction] Restrictions from these rights are permissible where they are provided by law and necessary in a democratic society for reasons of state security, public safety, the monetary interests of the state or the prevention and suppression of criminal offences, or protecting the data subject or the rights and freedoms of others<sup>47</sup>

[Remedy] Appeal to the data protection or other competent authority; judicial remedy.

[Example] Personal data collected by cookies or other technologies can be processed to build profiles of an Internet user's personal characteristics (gender, age, race, health information, physical information or else), online interests, preferences, behaviours and attitudes with the intention of offering personalised/targeted content or services (profiling) such as advertisement. The collection and processing of personal data in the context of profiling should be lawful, fair, for specified and legitimate purposes and proportionate.

---

<sup>46</sup> Recommendation [CM/Rec\(2010\)13](#) of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling , section 5

<sup>47</sup> Ibid., section 6.



## **ONLINE LIBERTY AND SECURITY**

*[Right]* Everyone has a right to be protected from criminal offences committed on or using the Internet including offences against the confidentiality, integrity and availability of computer data systems<sup>48</sup>, computer-related forgery and computer-related fraud<sup>49</sup> and other forms of crime (cyber harassment, cyber bullying, viruses, and denial of service attacks).

*[Restrictions]* Any security measure targeting the protection of the individual or the technical functioning of the Internet must be consistent with the standards of the ECHR, in particular article 8 and 10. Security measures that restrict another human right are only permissible in specific and narrowly defined circumstances that fulfill the conditions laid down in that specific right. No restrictions outside of these limits are permitted.

*[Remedies]* Different forms of recourse may be available such as reporting alleged illegal activities to Internet service providers and platforms which should implement readily accessible means/tools for users' reporting. Internet users should be also able to report alleged crimes to helplines established by civil society or competent state authorities and to report/appeal to the police and/or the prosecutor's office.

The state must provide for effective access to police and competent authorities in cases where users claim to be the victim of a crime on the internet. If the claim is found reasonable, the state must provide for access to remedy. As a last recourse the user must be afforded easy access to file a complaint with the national courts, and if national remedies are exhausted, to file an application with the ECtHR.

*[Example]* Individuals may find themselves exposed to cyber harassment, cyber bullying, viruses, denial of service attacks, credit card frauds, identity theft, etc.

## **RIGHT TO ONLINE ASSEMBLY AND ASSOCIATION**

*[Right]* Everyone has the right to peacefully meet and associate with others on the Internet regardless of the platform/website/application used for these purposes. This includes the right of Internet users to peacefully protest online and organise themselves.

*[Restrictions]* No other restrictions on these rights shall be placed other than those which are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. This shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.

*[Remedies]* Providers of Internet platforms shall implement readily accessible means of communication for users to report on unreasonable restrictions in the right to peacefully meet and associate on the internet.

The state must provide for effective and readily accessible means of recourse in cases where users claim to be unreasonably restricted from the right to peacefully meet and associate on the internet. If the restriction is found to be unreasonable, the state must provide for remedy. As a last recourse the user shall be afforded easy access to raise a complaint with the national courts, and if national remedies is exhausted, to the ECtHR.

*[Example]* to be completed.

---

<sup>48</sup> Budapest Convention on Cybercrime Chapter 2, title 1.

<sup>49</sup> Ibid, title 2.

## **FREEDOM OF RELIGION**

*[Right]* the Internet user has the right to manifest his/her religion or belief via the Internet, including teaching and practicing religion.

*[Restrictions]* on this rights should be in full compliance with conditions provided in Article 9 of the ECHR prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.

*[Remedies]* appeal to competent administrative (ombudsperson) and judicial authorities, the ECtHR.

*[Example]* to be completed.

## **RIGHT TO EDUCATION**

*[Right]* The right to education applies to the Internet. Everyone is entitled to use the Internet as a medium for education purposes and to access and use educational materials and other digital information for non-commercial purposes, education and research in compliance with the legal framework on copyright.

*[Restriction]*

*[Example]* to be completed.

*[Remedies]* complains to Internet/online service providers, to competent administrative authorities, judicial remedy.

## **RIGHTS OF PEOPLE WITH DISABILITIES**

*[Right]* Internet users with disabilities are entitled to an accessible Internet and information and communication technologies.<sup>50</sup>

*[Restrictions]*

*[Remedies]* The right to complain to responsible public authorities, Internet service providers, content providers, webmasters, domestic and roaming providers (defined in Regulation (EU) No 531/2012, Art 2 a, b), National Regulatory Authority in the telecommunications domain.

*[Example]* The newly adopted international standard ISO/IEC 40500, 2012 [Web Content Accessibility Guidelines (WCAG) 2.0] covers a wide range of recommendations for making web content more accessible. Following these guidelines the content will be accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech

---

<sup>50</sup> Principle of prohibition of discrimination , ECHR Prot 12, Article 1 “The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.” Article 9 of the UN Convention on the Rights of Persons with Disabilities and the new Article 8B added to the International Telecommunication Regulations (ITRs) agreed to at WCIT-12 in Dubai. Rule of the Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union (where data roaming services are included).



disabilities, photo-sensitivity and combinations of these. These guidelines can help making the Web content more usable to users in general.

Flash sites with visually attractive and interactive layouts are not accessible for screen readers that allow blind or visually impaired users to read the text that is displayed on the computer screen with a speech synthesizer.

### **RIGHTS OF THE CHILD**

#### ***[Right]***

- (1) Every child has a right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds through any media including the Internet.<sup>51</sup>
- (2) Children are entitled to special care and assistance on the Internet, in particular with regard to risk of harm which may arise from content and behaviour, such as online pornography, the degrading and stereotyped portrayal of women, the portrayal and glorification of violence and self-harm, demeaning, discriminatory or racist expressions or apologia for such conduct, solicitation (grooming), the recruitment of child victims of trafficking in human beings, bullying, stalking and other forms of harassment, which are capable of adversely affecting the physical, emotional and psychological well-being of children.<sup>52</sup>
- (3) Every child has the right to be protected from being recruited, caused or coerced into participating in pornographic performances made accessible or available on the Internet (for example through webcams).<sup>53</sup>
- (4) Every child has the right to be protected from the intentional causing to witness sexual abuse or sexual activities even without having to participate.<sup>54</sup>
- (5) Every child has the right to be protected from solicitation through the use of the Internet or other information and communication technologies for the purpose of engaging in sexual activities with the child (grooming) who, according to the relevant provisions of national law, has not reached the legal age for sexual activities and for the purpose of producing child pornography.<sup>55</sup>

***[Restriction]*** 1 and 2 are subject to restrictions permissible under Article 10, para. 2, whereas 3-4 are non-derogable rights.

The exercise of the right to freedom of expression right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary to protect the well-being of children. Any restriction would have to fulfil the conditions in Article 10(2) of the ECHR and the relevant ECtHR case law.<sup>56</sup>

---

<sup>51</sup> Convention on the Rights of the Child, Art. 13.

<sup>52</sup> 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

<sup>53</sup> Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No.: 201, Art.21, see also explanatory report on this point.

<sup>54</sup> Ibid., Art.22.

<sup>55</sup> Ibid., Art. 23.

<sup>56</sup> The needs and concerns of children online should be addressed without undermining the benefits and opportunities offered to them on the Internet (Note Parliamentary Assembly Recommendation 1882 (2009) on

*[Remedy]* Different forms of recourse may be available such as reporting alleged forms of sexual abuse of children on the Internet to Internet service providers and platforms which should implement readily accessible means for users' reporting. Internet users should be able to report alleged crimes to helplines established by civil society or competent state authorities and report/appeal to the police and/or the prosecutor's office. The state must provide for effective access to police and competent authorities in cases where users claim to be the victim of a crime on the internet. If the claim is found reasonable, the state must provide for access to remedy. As a last recourse the user must be afforded easy access to file a complaint with the national courts, and if national remedies are exhausted, to the ECtHR.

*[Example] to be completed.*

### **PROTECTION OF PROPERTY**

Article 1 of Protocol 1 of the ECHR provides:

"Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties."

### **RIGHT TO AN EFFECTIVE REMEDY**

*[Right]* Every one whose rights and freedoms as set forth in the ECHR and other Council of Europe standards are violated has the right to an effective remedy including the possibility of appeal to an Internet and/or online service provider through the procedures provided by them, alternative dispute resolution entities, independent supervisory authorities and judicial authorities.

The remedy must be available, accessible, generally known, reasonable in duration, effective in law and in practice, enabling effective investigation of a violation and access to an investigation procedure, capable of dealing with the substance of an arguable complaint, enforcing the substance of right recognised by the ECHR and granting appropriate relief and/or compensation as appropriate to those whose rights have been violated.

Every Internet user is entitled to ask and receive from Internet and online service providers information regarding the means of redress available to him.

*[Restriction]* not applicable

*[Remedy]* not applicable

*[Example]*

- Clear, consistent and transparent information regarding the means of redress available to the Internet user, which might be included in Terms of Use and/or Service or other guidelines and policies of Internet service/online providers;
- Channels/links/mechanisms/tools to contact Internet service/online providers with questions, issues, requests for information and reports of violations of rights as well as information about the policy for responding to such questions and requests;
- Mechanisms/tools provided by an Internet service/online provider to appeal decision/action taken by them;
- Due process for responses to appeals including promptness of response, information why decision/action was taken, etc.
- Filing complaint with a help-line/hotline;
- Appeal to consumer protection associations;
- Appeal to competent authority, ombuds-institutions;
- Appeal to a competent court/administrative tribunal;
- Appeal to ECtHR.