GUIDE TO HUMAN RIGHTS FOR INTERNET USERS

Legal instruments

Recommendation CM/Rec(2014)6
and explanatory memorandum

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Recommendation CM/Rec(2014)6
of the Committee of Ministers to member States
on a Guide to human rights for Internet users

(Adopted by the Committee of Ministers on 16 April 2014
at the 1197th meeting of the Ministers' Deputies)

1. Council of Europe member States have the obligation to secure for everyone within their jurisdiction the human rights and fundamental freedoms enshrined in the European Convention on Human Rights (ETS No. 5, the Convention). This obligation is also valid in the context of Internet use. Other Council of Europe conventions and instruments, which deal with the protection of the right to freedom of expression, access to information, the right to freedom of assembly, protection from cybercrime and of the right to private life and to the protection of personal data, are also applicable.

2. The obligations of States to respect, protect and promote human rights include the oversight of private companies. Human rights, which are universal and indivisible, and related standards, prevail over the general terms and conditions imposed on Internet users by any private sector actor.

3. The Internet has a public service value. People, communities, public authorities and private entities rely on the Internet for their activities and have a legitimate expectation that its services are accessible, provided without discrimination, affordable, secure, reliable and ongoing. Furthermore, no one should be subjected to unlawful, unnecessary or disproportionate interference with the exercise of their human rights and fundamental freedoms when using the Internet.

4. Users should receive support to understand and effectively exercise their human rights online when their rights and freedoms have been restricted or interfered with. This support should include guidance on access to effective remedies. In light of the opportunities that the Internet provides for transparency and accountability in the conduct of public affairs, users should be empowered to use the Internet to participate in democratic life.

5. To ensure that existing human rights and fundamental freedoms apply equally offline and online, the Committee of Ministers recommends under the terms of Article 15.*b* of the Statute of the Council of Europe that member States:

5.1. actively promote the Guide to human rights for Internet users, as set out in the Appendix, among citizens, public authorities and private sector actors and take specific action regarding its application in order to enable users to fully exercise their human rights and fundamental freedoms online;

5.2. assess, regularly review and, as appropriate, remove restrictions regarding the exercise of rights and freedoms on the Internet, especially when they are not in conformity with the Convention in the light of the relevant case law of the European Court of Human Rights. Any restriction must be prescribed by law, necessary in a democratic society to pursue a legitimate aim and proportionate to the legitimate aim pursued;

5.3. ensure that Internet users have access to effective remedies when their rights and freedoms have been restricted or when they believe that their rights have been violated. This requires enhancing co-ordination and co-operation among relevant institutions, entities and communities. It also necessitates the engagement of and effective co-operation with private sector actors and civil society organisations. Depending on the national context, this may include redress mechanisms such as those provided by data protection authorities, national human rights institutions (such as ombudspersons), court procedures and hotlines;

5.4. promote co-ordination with other State and non-State actors, within and beyond the Council of Europe, with regard to the standards and procedures which have an impact on the protection of human rights and fundamental freedoms on the Internet;

5.5. encourage the private sector to engage in genuine dialogue with relevant State authorities and civil society in the exercise of their corporate social responsibility, in particular their transparency and accountability, in line with the "Guiding Principles on Business and Human Rights: implementing the United Nations 'Protect, Respect and Remedy' Framework". The private sector should also be encouraged to contribute to the dissemination of the guide;

5.6. encourage civil society to support the dissemination and application of the guide so that it provides an effective tool for Internet users.

Appendix to Recommendation CM/Rec(2014)6

Introduction

1. This guide is a tool for you, the Internet user, to learn about your human rights online, their possible limitations, and available remedies for such limitations. Human rights and fundamental freedoms apply equally offline and online. This principle includes respect for the rights and freedoms of other Internet users. The guide provides you with information about what rights and freedoms mean in practice in the context of the Internet, how they can be relied and acted upon, as well as how to access remedies. It is an evolving document, open to periodic updating.

2. This guide is based on the European Convention on Human Rights and other Council of Europe conventions and instruments that deal with various aspects of human rights protection. All Council of Europe member States have a duty to respect, protect and fulfil the rights and freedoms contained in the instruments that they have ratified. The guide is also inspired by the continuous interpretation of these rights and freedoms by the European Court of Human Rights and by other relevant legal instruments of the Council of Europe.

3. The guide does not establish new human rights and fundamental freedoms. It builds on existing human rights standards and enforcement mechanisms.[1]

Access and non-discrimination

1. Access to the Internet is an important means for you to exercise your rights and freedoms and to participate in democracy. You should therefore not be disconnected from the Internet against your will, except when it is decided by a court. In certain cases, contractual arrangements may also lead to discontinuation of service but this should be a measure of last resort.

2. Your access should be affordable and non-discriminatory. You should have the greatest possible access to Internet content, applications and services using the devices of your choice.

3. You should expect public authorities to make reasonable efforts and to take specific measures to facilitate your access to the Internet if you live in rural and geographically remote areas, are on a low income and/or have special needs or disabilities.

4. In your interactions with public authorities, Internet service providers and providers of online content and services, or with other users or groups of users, you must not be discriminated against on any grounds such as gender, race, colour, language, religion or belief, political or other opinion, national or social origin, association with a national minority, property, birth or other status, including ethnicity, age or sexual orientation.

Freedom of expression and information

You have the right to seek, receive and impart information and ideas of your choice, without interference and regardless of frontiers. This means:

1. you have the freedom to express yourself online and to access information and the opinions and expressions of others. This includes political speech, views on religion, opinions and expressions that are favourably received or regarded as inoffensive, but also those that may offend, shock or disturb others. You should have due regard to the reputation or rights of others, including their right to privacy;

[1] This guide is part of a recommendation adopted by the Committee of Ministers of the 47 member States of the Council of Europe. More detailed information explaining the guide can be found in the explanatory memorandum to the recommendation.

2. restrictions may apply to expressions which incite discrimination, hatred or violence. These restrictions must be lawful, narrowly tailored and executed with court oversight;

3. you are free to create, re-use and distribute content respecting the right to protection of intellectual property, including copyright;

4. public authorities have a duty to respect and protect your freedom of expression and your freedom of information. Any restrictions to this freedom must not be arbitrary, must pursue a legitimate aim in accordance with the European Convention on Human Rights such as, among others, the protection of national security or public order, public health or morals, and must comply with human rights law. Moreover, they must be made known to you, coupled with information on ways to seek guidance and redress, and not be broader or maintained for longer than is strictly necessary to achieve a legitimate aim;

5. your Internet service provider and your provider of online content and services have corporate responsibilities to respect your human rights and provide mechanisms to respond to your claims. You should be aware, however, that online service providers, such as social networks, may restrict certain types of content and behaviour due to their content policies. You should be informed of possible restrictions so that you are able to take an informed decision as to whether to use the service or not. This includes specific information on what the online service provider considers as illegal or inappropriate content and behaviour when using the service and how it is dealt with by the provider;

6. you may choose not to disclose your identity online, for instance by using a pseudonym. However, you should be aware that measures can be taken, by national authorities, which might lead to your identity being revealed.

Assembly, association and participation

You have the right to peacefully assemble and associate with others using the Internet. In practice, this means:

1. you have the freedom to choose any website, application or other service in order to form, join, mobilise and participate in social groups and assemblies whether or not they are formally recognised by public authorities. You should also be able to use the Internet to exercise your right to form and join trade unions;

2. you have the right to protest peacefully online. However, you should be aware that, if your online protest leads to blockages, the disruption of services and/or damage to the property of others, you may face legal consequences;

3. you have the freedom to use available online tools to participate in local, national and global public policy debates, legislative initiatives and public scrutiny of decision-making processes, including the right to sign petitions and to participate in policy making relating to how the Internet is governed.

Privacy and data protection

You have the right to private and family life on the Internet which includes the protection of your personal data and respect for the confidentiality of your correspondence and communications. This means:

1. you should be aware that, in using the Internet your personal data is regularly processed. This happens when you use services such as browsers, e-mail, instant messages, voice-over Internet protocols, social networks and search engines and cloud data storage services;

2. public authorities and private companies have an obligation to respect specific rules and procedures when they process your personal data;

3. your personal data should only be processed when laid down by law or when you have consented to it. You should be informed of what personal data are processed and/or transferred to third parties, when, by whom and for what purpose. Generally, you should be able to exercise control over your personal data (check its accuracy, request a correction, a deletion or that personal data is kept for no longer than necessary);

4. you must not be subjected to general surveillance or interception measures. In exceptional circumstances, which are prescribed by law, your privacy with regard to your personal data may be interfered with, such as for a criminal investigation. Accessible, clear and precise information about the relevant law or policy and your rights in this regard should be made available to you;

5. your privacy must also be respected in the workplace. This includes the confidentiality of your private online correspondence and communications. Your employer must inform you of any surveillance and/or monitoring carried out;

6. you can be assisted by data protection authorities, which exist in a vast majority of European countries, to ensure that data protection laws and principles are upheld.

Education and literacy

You have the right to education, including access to knowledge. This means:

1. you should have online access to education and to cultural, scientific, scholarly and other content in official languages. Conditions might apply to such access in order to remunerate rights' holders for their work. You should also be able to freely access publicly funded research and cultural works in the public domain on the Internet, where available;

2. as part of Internet and media literacy you should have access to digital education and knowledge in order to exercise your rights and freedoms on the Internet. This includes skills to understand, use, and work with a broad range of Internet tools. This should enable you to critically analyse the accuracy and trustworthiness of content, applications and services that you access or wish to access.

Children and young people

As a child or young person, you have all the rights and freedoms outlined in this guide. In particular, because of your age, you are entitled to special protection and guidance when using the Internet. This means:

1. you have the right to freely express your views and participate in society, to be heard and to contribute to decision making on matters affecting you. Your views must be given due weight in accordance with your age and maturity and without discrimination;

2. you can expect to receive information in a language appropriate for your age and training from your teachers, educators and parents or guardians about safe use of the Internet, including about how to preserve your privacy;

3. you should be aware that content you create on the Internet or content concerning you created by other Internet users may be accessible worldwide and could compromise your dignity, security and privacy or be otherwise detrimental to you or your rights now or at a later stage in your life. Upon your request, this should be removed or deleted within a reasonably short period of time;

4. you can expect clear information about online content and behaviour that is illegal (for example online harassment) as well as the possibility to report alleged illegal content. This information should be adapted to your age and circumstances and you should be provided with advice and support with due respect for your confidentiality and anonymity;

5. you should be afforded special protection from interference with your physical, mental and moral welfare, in particular regarding sexual exploitation and abuse on the Internet and other forms of cybercrime. In particular, you have the right to education to protect yourself from such threats.

Effective remedies

1. You have the right to an effective remedy when your human rights and fundamental freedoms are restricted or violated. To obtain a remedy, you should not necessarily have to pursue legal action straight away. The avenues for seeking remedies should be available, known, accessible, affordable and capable of providing appropriate redress. Effective remedies can be obtained directly from Internet service providers, public authorities and/or national human rights institutions. Effective remedies can – depending on the violation in question – include inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation. In practice, this means:

1.1. your Internet service provider, providers of access to online content and services, or other company and/or public authority should inform you about your rights, freedoms and possible remedies and how to obtain them. This includes easily accessible information on how to report and complain about interferences with your rights and how to seek redress;

1.2. additional information and guidance should be made available from public authorities, national human rights institutions (such as ombudspersons), data protection authorities, citizens' advice offices, human rights or digital rights associations or consumer organisations;

1.3. national authorities have an obligation to protect you from criminal activity or criminal offences committed on or using the Internet, in particular when this concerns illegal access, interference, forgery or other fraudulent manipulation of your digital identity, computer and data contained therein. The relevant law-enforcement authorities have an obligation to investigate and take appropriate action, including seeking sanctions, if you complain of damage to, or interference with, your personal identity and your property online.

2. In the determination of your rights and obligations or of any criminal charge against you with regard to the Internet:

2.1. you have the right to a fair trial within a reasonable time by an independent and impartial court;

2.2. you have the right to an individual application to the European Court of Human Rights after exhausting all available domestic remedies.

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

CM Documents

CM(2014)31 addfinal 16 April 2014[1]

Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum

Introduction

1. The Internet plays an important role in people's daily life and in all aspects of human society. It is continually evolving and providing citizens with possibilities to access information and services, to connect and to communicate, as well as to share ideas and knowledge globally. The impact of the Internet on social, economic and cultural activities is also growing.

2. There is an increasing number of cases which relate to the Internet before the European Court of Human Rights ("the Court").[2] The Court has affirmed that "[t]he Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest."[3]

3. The Council of Europe's Internet Governance Strategy 2012-2015 attaches importance to the rights of Internet users. The chapter 'Maximising Rights and Freedoms for Internet Users', which aims at promoting access to and best use of the Internet includes as a line of action: "drawing up a compendium of existing human rights for Internet users to help them in communicating with and seeking effective recourse to key Internet actors and government agencies when they consider their rights and freedoms have been adversely affected: to report an incident, lodge a complaint or seek a right to reply, redress or other form of recourse".

Background and context

4. The Steering Committee on Media and Information Society (CDMSI), at its 1st meeting on 27-30 April 2012, proposed to the Committee of Ministers to set up a Committee of Experts on Rights of Internet Users (MSI-DUI) and agreed to its draft terms of reference. Further to the CDMSI's proposal, the Committee of Ministers approved the terms of reference at the 1147th meeting of the Ministers' Deputies on 6 July 2012.[4] The expected result of the MSI-DUI, according to its terms of reference, is:

> "*A compendium of existing human rights for Internet users is prepared to help them understand and exercise their rights when, considering their rights and freedoms have been adversely affected, they communicate with and seek effective recourse from key Internet actors and government agencies (2013)" (hereinafter the Compendium)*.

5. The MSI-DUI held its first meeting on 13 and 14 September 2012, in Strasbourg. It was agreed that the objective of the MSI-DUI work should not be to create new human rights but to examine the application of existing rights with regard to the Internet. The MSI-DUI decided to collect information, by means of a questionnaire sent to their networks and communities, on practical problems experienced by users, and thereby on possible violations of their human rights as well as available remedies.

[1] This document has been classified restricted until examination by the Committee of Ministers.
[2] For an overview of the European Court of Human Rights' case-law relating to the Internet please visit the factsheet on new technologies, October 2013.
[3] See Yildirim v. Turkey, no 3111/10 § 54.
[4] See CM(2012)91.

6. Consultations with stakeholders were held at the Internet Governance Forum (6 to 9 November 2012, Baku) in the workshop "Empowerment of Internet Users – which tools?". The participating MSI-DUI members used the outreach opportunities that this event offered to seek stakeholders' feedback on various topics relevant to the Compendium. Workshop discussions highlighted problems encountered by Internet users such as removal of user generated content without due process, issues related to personal data protection and the lack of effective remedies.

7. The MSI-DUI held its second meeting on 13 and 14 December 2012, in Strasbourg. It considered the replies received by different stakeholders on its questionnaire and discussed the information collected through its outreach to stakeholders. The MSI-DUI decided to complete the preliminary analytical phase of its work and, on this basis, to start drafting the Compendium; a first draft was outlined during this meeting.

8. At its third meeting, which took place on 20 and 21 March 2013 in Strasbourg, the MSI-DUI examined in detail issues related to the right to freedom of expression, the right to private life, freedom of assembly and association, online security, the right to education, the rights of the child, non-discrimination and the right to an effective remedy. This examination was based on relevant Council of Europe binding and non-binding standards and the case law of the Court. The MSI-DUI also discussed the type of instrument which the Council of Europe could adopt to endorse the Compendium, such as a Committee of Ministers' declaration or recommendation. The instrument should meet the twofold objective of providing Internet users with simple and clear guidance on their human rights online and ensuring adoption by member States of a text that is in line with their obligations under the European Convention on Human Rights (ECHR) and other Council of Europe standards.

9. The CDMSI at its third meeting, which took place from 23 to 26 April 2013, in Strasbourg, took the view that the Compendium should combine formal and simplified language, while paying due attention to avoiding over-simplification of existing human rights standards and jurisprudence of the Court. Discussions highlighted also the desirability to update the Compendium regularly in order to reflect the rapidly evolving Internet policies. The CDMSI also decided to submit comments on the draft Compendium, as it stood at the time of the consultations, noting that it was a 'work-in-progress' document, in order to provide overarching guidance and orientation. The replies received supported the approach taken by the MSI-DUI to prepare a user-friendly awareness-raising document that gave special attention to the right to freedom of expression, the right to private life, the right to education, the rights of the child and protection from cybercrime.

10. The draft Compendium was presented to and discussed with stakeholders at the European Dialogue on Internet Governance (EuroDIG, 20-21 June 2013 in Lisbon) notably in the workshop "Towards a Human Internet? Rules, Rights and Responsibilities for our Online Future". An informal meeting was held in Lisbon among MSI-DUI members who attended the workshop. It was considered that the draft Compendium should be shortened with a view to being more accessible by Internet users. Following these discussions, as well as inter-sessional work of MSI-DUI members, an ad hoc meeting of available MSI-DUI members was held on 10 September 2013, in Strasbourg. The MSI-DUI examined a draft Committee of Ministers' recommendation on human rights for Internet users, which included in its appendix a draft Compendium of human rights and fundamental freedoms for Internet users. The draft Compendium adopted an approach which addresses the user directly. In view of this approach, it was decided to re-entitle the Compendium as a "Guide on Human Rights for Internet Users".

11. At its last meeting, held on 1 and 2 October 2013, in Strasbourg, the MSI-DUI examined and finalised its proposals to the CDMSI for a draft Committee of Ministers recommendation on a Guide to Human Rights for Internet Users (hereinafter the Guide). It agreed to hold multi-stakeholder consultations, including a Council of Europe Open Forum on the Guide during the Internet Governance Forum (22-25 October 2013, Indonesia). A number of selected stakeholders, representing the private sector, civil society, the technical community and academia were asked to provide their comments and suggestions on the Guide. In addition, informal comments and feedback on the draft recommendation were invited from other relevant Council of Europe steering committees, including the Steering Committee for Human Rights (CDDH), the European Committee on Legal Cooperation (CDCJ), the European Committee on Crime Problems (CDPC), as well as conventional

committees including the Consultative Committee of the Convention for the *Protection* of Individuals with regard to Automatic Processing of Personal Data *(*T-PD*),* the Cybercrime Convention Committee (T-CY), the Committee of Experts on Terrorism (CODEXTER) and the Committee of Parties to the Convention on the protection of children against sexual exploitation and sexual abuse (T-ES). In response, the CDDH, the CDCJ, and members of the T-PD Bureau all provided comments that were then taken into consideration and integrated into the draft Recommendation and draft Explanatory memorandum by the CDMSI.

12. In addition, around 30 contributions were received from representatives of the private sector (telecommunications companies, online service providers), key civil society organisations, the technical community as well as academicians from different parts of the world. They generally welcomed the Council of Europe's work on the draft Guide and provided numerous comments and proposals for changes thereto.

13. The CDMSI, during its 4th meeting which was held from 3 to 6 December 2013, examined the proposals of the MSI-DUI for a draft Committee of Ministers recommendation on a Guide on human rights for Internet users. It took note of the multi-stakeholder consultations mentioned above and finalised the draft recommendation on the basis of final comments which were sent by e-mail.

Comments on Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users

14. The aim of this recommendation is to foster the exercise and protection of human rights and fundamental freedoms on the Internet in all Council of Europe member States. Individuals' and communities' access to the Internet and best use of it necessitate efforts to inform and empower them to exercise their rights and freedoms in online environments. This approach had been affirmed by the Committee of Ministers in its Declaration on Internet Governance Principles, of 2011, in which it underlined its vision of a people-centred and human rights based approach to the Internet which empowered Internet users to exercise their rights and freedoms on the Internet as a principle of Internet governance.

15. The Guide, which is annexed to this recommendation, offers some basic information on selected human rights in the ECHR and from other relevant Council of Europe standards. It focuses on particular rights and freedoms and related international law standards, in particular regarding the right to freedom of expression, freedom of assembly and association, the right to privacy and protection of personal data, children's rights, and the right to an effective remedy. It has been drafted in a language that is easy for users to understand. To keep the text as simple as possible, the MSI-DUI decided not to refer to the strict legal wording of member States' obligations in international law, including the case law of the Court.

16. Human rights and fundamental freedoms are guaranteed in various Council of Europe instruments which are applicable both to offline and online environments, thus not exclusively to the Internet. Notably, human rights and fundamental freedoms are enshrined in the ECHR which is interpreted by the Court in its case law. A number of Council of Europe conventions and other non-binding instruments offer additional explanation and orientation for Internet users. The MSI-DUI considered that in order for Internet users to understand their rights and freedoms there was a need to explain in simple wording relevant international law standards of the Council of Europe and the United Nations.

Preamble

17. The preamble sets out the reasons that led the Committee of Ministers to adopt the recommendation to its member States. The premise for the recommendations is that the responsibility to safeguard human rights and fundamental freedoms lies with the Council of Europe member States. This must be done in compliance with the ECHR as interpreted by the Court. Other legally binding instruments of the Council of Europe are also relevant, notably the Convention on Cybercrime (hereinafter the 'Budapest Convention'), the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, hereinafter the 'Lanzarote Convention'), and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No.108, hereinafter 'Convention 108').

18. Other non-binding standards adopted by the Committee of Ministers provide guidance to member States on Internet related matters, including: Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet; 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; 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; Recommendation CM/Rec (2011)7 of the Committee of Ministers to member States on a new notion of media; 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; and Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines.

19. The second paragraph of the preamble specifies that the obligations of States to respect, protect and promote human rights engender the oversight of private companies. This statement is derived from Article 1 of the ECHR according to which States shall secure to everyone within their jurisdiction the rights and freedoms set forth in the Convention. This includes protection against human rights violations by non-State actors and requires taking appropriate steps to prevent, investigate, punish and redress violations through effective legislation and measures. The Court has affirmed in its judgments that States have positive obligations to protect the fundamental rights and freedoms of individuals on the Internet, notably as regards freedom of expression[5], the protection of children and young people[6], the protection of morals and the rights of others[7], combating racist or xenophobic discourse, and in addressing discrimination and racial hatred[8]. In addition, the Court has held States accountable for failing to protect their citizens from adverse effects on their rights and freedoms resulting from actions of private companies.[9] The second paragraph also echoes the principle of universality and indivisibility of human rights, which is based on the Vienna Declaration issued at the Summit conference of Heads of State and Government of the member States of the Council of Europe, which took place on 9 October 1993.

20. The third paragraph of the preamble reaffirms the public service value of the Internet as set out in the relevant Committee of Ministers' Recommendation CM/Rec(2007)16.[10] Considering the important role that the Internet plays in users' everyday activities and the need to ensure the protection of their human rights on the Internet, the recommendation emphasises that people must not be subject to unlawful, unnecessary and disproportionate interferences with the exercise of their rights and freedoms.

21. The fourth paragraph of the preamble defines the objective of the recommendation to foster users' understanding and promote the effective exercise of human rights online, including access to effective remedies. Informing users about the risks to their fundamental rights and freedoms and the possibilities for redress are therefore important. The statement regarding the opportunities provided by the Internet for transparency and accountability in public affairs explains an element of the rationale of the recommendation that is empowering individuals and communities to participate in democratic life.

[5] See Özgür Gündem v. Turkey, no. 23144/93, §§ 42-46.
[6] K.U. v. UK, no 2872/02.
[7] Pay v. UK, no. 32792/05.
[8] Féret v. Belgium no.15615/07.
[9] López Ostra v. Spain, no. 16798/90, § 44-58; Taşkin and Others v. Turkey; Fadeyeva v. the Russian Federation. In Khurshid Mustafa and Tarzibachi v. Sweden no 23883/06 the Court found that a domestic court's interpretation of a private act (contract) engaged the responsibility of the respondent State, thus broadening the scope of Article 10 protection to restrictions imposed by private persons.
[10] Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet.

Operative part of the recommendation

22. Paragraph 5 States a key principle of the Council of Europe's Internet-related standards, that is fundamental rights and freedoms apply equally to online and offline environments[11]. This approach has also been affirmed by the United Nations Human Rights Council in its Resolution of 2012 on "The Promotion, Protection and Enjoyment of Human Rights on the Internet". Promoting the application of the Guide will reinforce the protection of human rights and fundamental freedoms in compliance with existing human rights standards.

23. Sub-paragraph 5.1, recommends to member States that the Guide should be promoted not only by public authorities but also via the private sector. This could include its publication and dissemination in printed formats or adaptations in electronic formats. Relevant public authorities could also make it available on their websites. The private sector could be encouraged to do the same.

24. Sub-paragraph 5.2, reaffirms that the exercise of human rights and fundamental freedoms on the Internet may be subject to restrictions which pursue legitimate aims and are necessary in a democratic society as stipulated in the relevant articles of ECHR. In order to ensure compliance with these conditions the Committee of Ministers recommended to its member States to assess, regularly review and where appropriate remove restrictions with human rights and fundamental freedoms on the Internet.

25. Sub-paragraph 5.3, calls on member States to enhance their efforts to guaranteeing the right to an effective remedy, *inter alia*, by ensuring enhanced co-ordination and co-operation among existing relevant institutions, entities (including regulators for electronic communications) and communities which offer redress mechanisms, such as in the context of processing complaints lodged by Internet users. The recommendation also acknowledges that there is a diversity of redress mechanisms available in different member States, such as data protection authorities, ombudspersons, court procedures, or hotlines. Member States could also conduct an audit of existing redress mechanisms in their jurisdictions and compile the relevant information in a user-friendly inventory of redress mechanisms. Such information could be disseminated together with the Guide, for example in the form of an appendix. This is one of the follow-up actions which may be taken further to the adoption of the recommendation.

26. By its very nature, the Internet operates by sending and receiving requests for information across borders and therefore regardless of frontiers. This means that human rights and fundamental freedoms on the Internet in member States may be exposed to action by State or non-State actors beyond the Council of Europe's borders; for example freedom of expression and access to information, as well as privacy with regard to personal data can be interfered with. Therefore, sub-paragraph 5.4, recommends co-ordination between Council of Europe member States and non-Council of Europe member States as well as non-State actors.

27. Sub-paragraph 5.5, recommends to member States to encourage genuine dialogue between the private sector and relevant State authorities as well as civil society as regards the exercise of the latter's social responsibility. A foundational principle of the Guiding Principles on Business and Human Rights[12] is that business enterprises should respect human rights, which means that they should avoid infringing on the human rights of others and address adverse human rights impact with which they are involved. The transparency and accountability of private sector actors is emphasised as an important means of demonstrating their responsibility as is actively promoting and disseminating it. For example, Internet service providers and content access providers could make references to the Guide in the terms and conditions of use of their services.

[11] See Committee of Ministers Declaration on Internet Governance Principles, principle 1 "Human Rights, Democracy and Rule of "

[12] Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (A/HRC/17/31) endorsed by the Human Rights Council by Resolution Human rights and transnational corporations and other business enterprises A/HRC/RES/17/4. In particular the Guiding Principles provide that States should enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps; ensure that other laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights; provide effective guidance to business enterprises on how to respect human rights throughout their operations; encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts.

28. Sub-paragraph 5.6, acknowledges the key contribution that the civil society can give in promoting the Guide and compliance with it. Therefore, it is recommended that member States encourage civil society organisations and activists to help in the dissemination and application of the Guide and rely on it when advocating for the implementation of human rights standards and compliance with them.

Appendix to Recommendation CM/Rec(2014)6

Guide to Human Rights for Internet Users

Introduction

29. The Guide addresses the user directly. It is a tool for the Internet user who is any individual who does not have specialised knowledge about the Internet which is based on education or training. In particular, it focuses on the user's ability to manage their activities on the Internet (e.g. their identity, their personal data). They should be fully informed about the different choices they make on the Internet which may affect their rights and freedoms and the consequences of giving their consent to such choices. They should understand the limitations of their rights. They should be aware of the redress mechanisms available to them.

30. The Guide is based on the ECHR and the relevant jurisprudence of the Court. It also draws from other legally-binding Council of Europe instruments. Other instruments are also relied upon, in particular certain declarations and recommendations of the Committee of Ministers. The Guide is without prejudice to the enforceability of existing human rights standards on the basis of which it has been elaborated. The rights and freedoms in the Guide are enforceable under the legal instruments on the basis of which they are elaborated. The Guide refers to existing human rights standards and the relevant mechanisms for their enforcement, and does not establish new rights and freedoms. The Guide is neither an exhaustive nor a prescriptive explanation of human rights standards. For example, further clarifications on possible restrictions and interferences with human rights, and guidance on helping users deal with violence and abuse on the Internet, could merit further attention in order to help users understand their rights and to protect themselves and others. However, the Guide remains open to updating in order to keep pace with new standards of the Council of Europe and the case law of the Court as technology develops.

Access and non-discrimination

31. The Guide emphasises principles and considerations which are deemed to be intrinsically linked and generally applicable to all the human rights and fundamental freedoms contained in it, including access to the Internet and the principle of non-discrimination.

32. Although access to the Internet is not yet formally recognised as a human right (noting differences in national contexts including domestic law and policy), it is considered as a condition and an enabler for freedom of expression and other rights and freedoms[13]. Consequently, the disconnection of an Internet user could adversely affect the exercise of her/his rights and freedoms and could even amount to a restriction of the right to freedom of expression, including the right to receive and impart information. The Court has stated that the Internet has become today one of the principal means for the exercise of the right to freedom of expression and information by individuals. Freedom of expression applies not only to the content of information but also to the means of its dissemination, since any restriction imposed on the latter necessarily interferes with the right to receive and impart information. Such interferences can only be accepted if they meet the conditions

[13] The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue has emphasised that "the Internet has become an indispensable tool for realising a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet widely available, accessible and affordable to all segments of population." "[B]y acting as a catalyst for individuals to exercise their right to freedom of opinion and expression the Internet also enables the realisation of a range of other human rights" http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf.

stated in Article 10, paragraph 2 of the ECHR as interpreted by the Court.[14] A measure that is bound to have an influence on the individuals' accessibility of the Internet engages the responsibility of the State under Article 10.[15]

33. Against this background, the Guide states that Internet users should not be disconnected against their will except when it is decided by a court. This, however, should not be understood as pre-empting legitimate disconnection measures such as in the context of obligations stemming from contractual obligations. Internet consumers who do not pay for their service may be disconnected from the Internet. However this should be a measure of last resort. Moreover, children can be subjected to discontinuation of access to the Internet in the context of exercise of parental control over Internet usage of the Internet, depending on the child's age and maturity.

34. Internet users should have effective remedies against measures of disconnection from the Internet when this is not decided by a court. This includes Internet service providers informing Internet users about the grounds and legal basis for the disconnection measure and the procedures for objecting to it and requesting reinstatement of full access to the Internet. Such requests should be treated within reasonable time limits. Moreover, every Internet user, in the exercise of his right to fair trial, should be able to request a review of the disconnection measure by a competent administrative and/or judicial authority. These due process aspects are summarised in the last section of the Guide, which is entitled "Effective Remedies".

35. Positive action or measures taken by State authorities to ensure that everyone is connected to the Internet is another dimension of the issue of access to the Internet. The Committee of Ministers of the Council of Europe has recommended to its member States to promote the public service value of the Internet.[16] This is understood as "people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions) and the resulting legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing." This section informs the user that she/he should have Internet access which is affordable and non-discriminatory.

36. The right to access Internet content is linked to the right to receive and impart information on the Internet as referred to in Article 10 of the ECHR.[17] The Council of Europe's Committee of Ministers has affirmed that 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. This is a general principle commonly referred to as 'network neutrality' which should apply irrespective of the infrastructure or the network used for Internet connectivity.[18]

37. Public authorities should make reasonable efforts to facilitate access to the Internet for specific categories of individuals such as those living in remove areas and people with disabilities. This is based on the principle of universal community service which is laid down in Recommendation No.R(99)14 of the Committee of Ministers concerning new communication and information services.[19] It emphasises that individuals living in rural or geographically remote areas or those with low income or special needs or disabilities can expect specific measures from public authorities in relation to their Internet access.

[14] See note 2 above, § 50. See also Autronic AG v Switzerland (No. 12726/87). In Khurshid Mustafa and Tarzibachi v. Sweden no 23883/06 the Court found that a domestic court's interpretation of a private act (contract) engaged the responsibility of the respondent State, thus broadening the scope of Article 10 protection to restrictions imposed by private persons.
[15] See note 2 above, § 53.
[16] See note 9 above, CM/Rec(2007)16, section II.
[17] See note 2 above, § 50.
[18] Declaration of the Committee of Ministers on Network Neutrality, adopted by the Committee of Ministers on 29 September 2010. See also, 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.
[19] See note 9 above, CM/Rec(2007)16, appendix 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.

38. The expectations of people with disabilities to have equivalent and non-discriminatory access to the Internet as enjoyed by other Internet users is derived from instruments of the Council of Europe which recommend to member States to take action to foster the provision of adequate facilities for the access to the Internet and ICTs by disabled users.[20] Member States should promote affordable access bearing in mind the importance of design, the need to raise awareness among these persons and groups, the appropriateness and attractiveness of Internet access and services as well as their adaptability and compatibility. [21]

39. The principle of non-discrimination should apply to user interactions with public authorities, Internet service providers, content access providers and other companies, users, or other groups of users. The fourth paragraph is a paraphrasing of Article 14 of the ECHR and Article 1 of Protocol 12 of the ECHR, both concerning the prohibition on discrimination.

Freedom of expression and information

40. This section concerns the right to freedom of expression as enshrined in Article 10 of the ECHR. The Court has affirmed in its jurisprudence that Article 10 is fully applicable to the Internet.[22] The right to freedom of expression includes the right to freely express opinions, views, ideas and to seek, receive and impart information regardless of frontiers. Internet users should be free to express their political convictions as well as their religious and non-religious views. The latter concerns the exercise of the right to freedom of thought, conscience and religion as enshrined in Article 9 of the ECHR. Freedom of expression is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb.[23]

41. The exercise of the right to freedom of expression by Internet users' must be balanced with the right to protection of reputation. The Court has held in a number of cases that this is a right which is protected by Article 8 of the ECHR concerning the respect for private life.[24] The Court has found that, as a matter of principle, the rights guaranteed under Articles 8 and 10 deserve equal respect. It considers that where the right to freedom of expression is being balanced with the right to respect for private life, the relevant criteria in the balancing exercise include the following elements: contribution to a debate of general interest, how well known the person concerned is, the subject of the report, the prior conduct of the person concerned, the method of obtaining the information and its veracity, the content, form and consequences of the publication, and the severity of the sanction imposed.[25] Therefore, the Guide specifies that the Internet user should have due regard to the reputation of others, including their right to privacy.

42. There is expression that does not qualify for protection under Article 10 of the ECHR such as hate speech. The Court has found that certain forms of expression which amount to hate speech or which negate the fundamental values of the ECHR are excluded from the protections afforded by Article 10 of the Court.[26] In this connection the Court applies Article 17 of the ECHR. Although there is no universally acceptable definition of hate speech, the Council of Europe's Committee of Ministers has stated that the term "hate speech" shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism 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."[27] Paragraph 2 of the section on freedom of expression provides concise information which is formulated in simple language for the user with regard to the point that hate speech is not dealt with under Article 10 of the

[20] Ibid.
[21] See note 9 above, CM/Rec(2007)16, Appendix, section II.
[22] See note 2 above, §50.
[23] Handyside v. the United Kingdom, judgment of 7 December 1976, Series A No. 24, para.49.
[24] Chauvy and Others, no. 64915/01 § 70; Pfeifer v. Austria, no. 12556/03, § 35; and Polanco Torres and Movilla Polanco v. Spain, no. 34147/06, § 40.
[25] Delfi As v. Estonia, no. 64569/09, § 78-81 (this case has been referred to the Grand Chamber of the Court); Axel Springer AG v. Germany no. 39954/08 § 89-95, and Von Hannover v. Germany (no. 2), nos. 40660/08 and 60641/08 §§ 108-113.
[26] Féret v. Belgium no. 15615/07; Garaudy v. France no. 65831/01, 24.06.2003, admissibility decision; Leroy v. France no. 36109/03; Jersild v. Denmark no. 15890/89; Vejdeland and Others v. Sweden no. 1813/07.
[27] Recommendation No. R (97) 20 of the Committee of Ministers to member States on "Hate Speech"..

ECHR. This paragraph does not attempt to explain in legal terms the different ways in which article 10 and article 17 of the ECHR might apply to hate speech. Given the legal nature of this distinction it was considered that information on this point is more appropriate for the explanatory memorandum.

43. Users have the right to receive and impart information on the Internet, in particular to create, re-use and distribute content using the Internet. The Court has examined the relationship between intellectual property protection and freedom of expression in relation to cases of criminal conviction for copyright infringements. The Court has considered such convictions as interferences with the right to freedom of expression which in order to be justified must prescribed by law, pursue the legitimate aim of protecting the rights of others, and be considered necessary in a democratic society. [28] The sharing or allowing others to share files on the Internet, even copyright-protected material and for profit-making purposes, is covered by the right to receive and impart information as provided in Article 10 of the ECHR. [29]This is a right which is not absolute and so there is a need to weigh, on the one hand, the interest of sharing information with, on the other hand, the interest in protecting the rights of copyright holders. The Court has stressed that intellectual property benefits from the protection afforded by Article 1 of Protocol to the ECHR. Thus, it is a question of balancing two competing interests which are both protected by the ECHR.

44. The Committee of Ministers recommendation to its member States to promote the public service value of the Internet includes specific guidance on measures and strategies regarding freedom of communication and creation on the Internet regardless of frontiers. In particular, measures should be taken to facilitate, where appropriate, “re-uses” of Internet content, which means the use of existing digital content resources to create future content or services done in a manner that is compatible with respect for intellectual property rights.[30]

45. Paragraph 4 provides a general overview of the requirements that restrictions of the right to freedom of expression should meet. Member States have a primary duty, pursuant to Article 10 ECHR not to interfere with the communication of information between individuals, be they legal or natural persons. The Court has affirmed that the effective exercise of the right to freedom of expression may also require positive measures of protection, even in the sphere of relations between individuals. The responsibility of the State may be engaged as a result of failing to enact appropriate domestic legislation[31]. A violation of the ECHR can also be established where a national court’s interpretation of a legal act, be it a private contract, a public document, a statutory provision or an administrative practice, appears unreasonable, arbitrary, discriminatory or, more broadly, inconsistent with the underlying principles of the ECHR.[32]

46. Freedom of expression is not an absolute right and can be subjected to restrictions. Interferences with freedom of expression must be seen as any form of restriction coming from any authority exercising public power and duties or acting in the public service, such as courts, prosecutors’ offices, police, any law-enforcement body, intelligence services, central or local councils, government departments, army decision-making bodies, and public professional structures.

47. In compliance with Article 10, paragraph 2, of the ECHR, any interference must be prescribed by law. This means that the law must be accessible, clear and sufficiently precise to enable individuals to regulate their behaviour. The law should provide for sufficient safeguards against abusive restrictive measures, including effective control by a court or other independent adjudicatory body. [33] An interference must also 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. This list is exhaustive yet its

[28] Neij and Sunde Kolmisoppi v. Sweden no.40397/12. See also Ashby Donald and others v. France, no, 36769/08 § 34.
[29] Ibid.
[30] See note 9 above, CM/Rec(2007)16, Appendix, section III, second indent.
[31] Vgt Verein gegen Tierfabriken v. Switzerland, no. 24699/94, § 45.
[32] See Khurshid Mustafa and Tarzibachi v. Sweden no 23883/06 § 33; Plaand Puncernau v. Andorra, no. 69498/01, § 59, ECHR 2004-VIII.
[33] See note 2 above, § 64.

interpretation and scope evolves with the case law of the Court. An interference must also be necessary in a democratic society which means that it should be proven that there is a pressing social need for it, that it pursues a legitimate aim, and that it is the least restrictive means for achieving that aim.[34] These requirements are summarised in a language that is accessible for the user i.e. any restrictions to the freedom of expression must not be arbitrary and must pursue a legitimate aim in accordance with the ECHR such as among others, the protection of national security or public order, public health or morals and must comply with human rights law.

48. More detailed information about guarantees that should be afforded to Internet users when there are restrictions to the right to freedom of expression online are contained in the following paragraphs of the explanatory memorandum. Blocking and filtering are examples of such restrictions which may amount to violations of freedom of expression. Some general principles with regard to blocking and filtering are based on the Court case law or other relevant standards adopted by the Committee of Ministers[35].

49. Nationwide general blocking or filtering measures might be taken by State authorities only if the filtering concerns specific and clearly identifiable content, based on a decision on its illegality by a competent national authority which can be reviewed by an independent and impartial tribunal or regulatory body in accordance with the requirements of Article 6 of the ECHR.[36] State authorities should ensure that all filters are assessed both before and during their implementation to ensure that their effects are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unjustified blocking of content.[37]

50. Measures taken to block specific Internet content must not be arbitrarily used as a means of general blocking of information on the Internet. They must not have a collateral effect in rendering large quantities of information inaccessible, thereby substantially restricting the rights of Internet users.[38] They should be prescribed by law. There should be strict control of the scope of blocking and effective judicial review to prevent any abuse of power.[39] Judicial review of such a measure should weigh-up the competing interests at stake, strike a balance between them and determine whether there a less far-reaching measure could be taken to block access to specific Internet content.[40] The requirements and principles mentioned above 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.[41]

51. Filtering and de-indexation of Internet content by search engines entails the risk of violating the freedom of expression of Internet users. Search engines have freedom to crawl and index information available on the World Wide Web. They should not be obliged to monitor their networks and services proactively in order to detect possibly illegal content and should not conduct any ex-ante filtering or blocking activity unless mandated by a court order or by a competent authority. De-indexation or filtering of specific websites at the requests of public authorities should be transparent, narrowly tailored and reviewed regularly subject to compliance with due process requirements.[42]

52. This section also identifies some of the guarantees that Internet users should be afforded when restrictions apply, focusing notably on information to the user and possibilities to challenge these restrictions. This is referred to in the Council of Europe's Committee of Ministers recommendation on filtering and blocking measures. [43] Internet users should be given information about when filtering has

[34] Ibid. § 66-70.
[35] 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, see Appendix, part III, ii . See also, note 1 above.
[36] Ibid. CM/Rec(2008)6, see Appendix, part III, iv.
[37] Ibid.
[38] See note 2 above, § 52; 66- 68 and Committee of Ministers Declaration on Freedom of Communication on the Internet
[39] Ibid. note 2 above, § 64. Association Ekin v. France, n° 39288/98
[40] Ibid. note 2 above § 64-66.
[41] See Declaration on Freedom of Communication on the Internet, principle 3.
[42] See Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, Appendix, part III.
[43] See note 34 above, CM/Rec(2008)6, see Appendix, part I; Ibid, CM/Rec(2012)3, Appendix, part III.

been activated, why a specific type of content has been filtered and to understand how, and according to which criteria, the filtering operates (for example black lists, white lists, keyword blocking, content rating, de-indexation or filtering of specific websites or content by search engines). They should be given concise information and guidance regarding the manual overriding of an active filter, namely who to contact when it appears that content has been unjustifiably blocked and the means which may allow a filter to be overridden for a specific type of content or website. Users should be afforded effective and readily accessible means of recourse and remedy, including the suspension of filters, in cases where users claim that content has been blocked unjustifiably.

53. It is possible that companies, such as social networks, remove content created and made available by Internet users. These companies may also deactivate users' accounts (e.g. a user's profile or presence in social networks) justifying their action on non-compliance with their terms and conditions of use of the service. Such actions could constitute an interference with the right to freedom of expression and the right to receive and impart information unless the conditions of Article 10, paragraph 2 of the ECHR as interpreted by the Court, are met.[44]

54. According to the United Nations Guiding Principles on Business and Human Rights Business (which are not a binding instrument) enterprises have a responsibility to respect human rights, which requires them to avoid causing or contributing to adverse impacts on human rights and to provide for or cooperate in the remediation of such impacts. The duty to protect and to provide access to effective remedy is essentially incumbent on States. This is echoed in paragraph 5 of the section freedom of expression. The corporate social responsibility of online service providers includes a commitment to combating hate speech and other content that incites violence or discrimination. Online service providers should be attentive to the use of, and editorial responses to, expressions motivated by racist, xenophobic, anti-Semitic, misogynist, sexist (including as regards Lesbian Gay Bisexual and Transgender people) or other bias.[45] These providers should also be ready to help Internet users report content or expression of views and/or behaviour that may be considered illegal.[46]

55. The Guide alerts Internet users that online service providers that host user-created content are entitled to exercise different levels of editorial judgement over the content on their services.[47] Without prejudice to their editorial freedom, they should ensure that Internet users' right to seek, receive and impart information is not infringed upon in accordance with Article 10 of the ECHR.[48] This means that any restriction on user-generated content should be specific, justified for the purpose it is restricted, and communicated to the Internet user concerned.

56. The Internet user should be able to make an informed decision as to whether to use the online service or not. In practice, the Internet user should be fully informed about any foreseen measures to remove content created by her/him or to deactivate her/his account before these are taken.[49] Internet users should also be provided with accessible (in a language that the user understands), clear and precise information on the facts and grounds for taking measures on content removal and account deactivation. This includes the legal provisions on which they are based and other elements used to assess the proportionality and legitimacy of the aim pursued. They should also be able to request a review of the content removal and/or account de-activation, done within a reasonable time and subject to the possibility to complain against the decision to a competent administrative and/or judicial authority.

[44] Recommendation CM/Rec (2011)7 of the Committee of Ministers to member States on a new notion of media, §. 7, Appendix, § 15; 44-47; 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, § 3.
[45] Ibid., CM/Rec (2011)7, § 91.
[46] Ibid., CM/Rec(2012)4, II/10.
[47] Ibid., CM/Rec (2011)7, § 18; 30-31.
[48] Ibid., CM/Rec (2011)7, § 7, 2nd indent.
[49] See Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users, by Erica Newland, Caroline Nolan, Cynthia Wong, and Jillian York , available at: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pd.f

57. The sixth sub-paragraph concerns the issue of anonymity. This is based on the case law of the Court, the Budapest Convention and other instruments of the Committee of Ministers. The Court considered the issue of confidentiality of Internet communications in a case involving the failure of a Council of Europe member State to compel an Internet service provider to disclose the identity of a person who placed an indecent advertisement concerning a minor on an Internet dating website. The Court held that although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield, on occasion, to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. The State has a positive obligation to provide a framework which reconciles those competing interests.[50]

58. The Budapest Convention does not criminalise the use of computer technology for purposes of anonymous communication. According to its Explanatory Report, "the modification of traffic data for the purpose of facilitating anonymous communications (e.g. activities of anonymous remailer systems) or the modification of data for the purposes of secure communications (e.g. encryption) should in principle be considered a legitimate protection of privacy, and, therefore, be considered as being undertaken with right. However, Parties [to the Budapest Convention] may wish to criminalise certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime."[51]

59. The Council of Europe's Committee of Ministers affirmed the principle of anonymity in its Declaration on Freedom of Communication on the Internet.[52]Accordingly, in order to ensure protection against online surveillance and to enhance freedom of expression, Council of Europe member States should respect the will of Internet users not to disclose their identity. However, respect for anonymity does not prevent member States from taking measures in order to trace those responsible for criminal acts, in accordance with national law, the ECHR and other international agreements in the fields of justice and the police.

Assembly, association and participation

60. The right to freedom of assembly and association is enshrined in Article 11 of the ECHR. It also relates to the principles established by the Court regarding the protection of political speech, in particular that there is little scope under Article 10, paragraph 2 of the ECHR for restrictions of political speech or debates of questions of public interest.[53]

61. The user has the right to peacefully assemble and associate with others using the Internet. This includes forming, joining, mobilising and participating in societal groups and assemblies as well as in trade unions using Internet-based tools. This also includes for example the signing of a petition to participate in a campaign or other forms of civic action. The user should have the freedom to choose the tools for the exercise of the rights such as websites, applications or other services. The exercise of this right is not conditional upon any formal recognition of social groups and assemblies by public authorities.

62. The right to protest applies equally online and offline. Protests which have consequences for the general public, such as disruption or blocking of access to premises, fall within the limits of the exercise of freedom of assembly in accordance with Article 11 of the ECHR. However, this may not always be the case when such action gives rise to the disruption of online services, such as unauthorised access to a particular website or a restricted online space, or the handling of digital content without authorisation. Ultimately, it is important to apprise the user that the freedom and consequences of online protest, engendering disruption, may not be as freely accepted.

[50] K.U. v. Finland, no. 2872/02 § 49.
[51] Budapest Convention on Cybercrime, Article 2, Explanatory Report, §. 62.
[52] See Declaration on Freedom of Communication on the Internet, Principle 7.
[53] Wingrove v. the United Kingdom, 25 November 1996, § 58, Reports 1996-V.

63. The Internet has become a tool for citizens to actively participate in building and strengthening democratic societies. The Committee of Ministers has recommended that its member States should develop and implement strategies for e-democracy, e-participation and e-government using information and communication technologies (ICTs) in democratic processes and debates, both in relationships between public authorities and civil society as well as in the provision of public services. [54]

64. This includes the freedom to participate in local, national and global public policy debates, legislative initiatives as well as in the scrutiny of decision-making processes, including the right to sign petitions by means of using ICTs where they exist. This is based on Committee of Ministers' recommendations to its member States to encourage the use of ICTs by citizens (including online forums, weblogs, political chats, instant messaging and other forms of citizen-to-citizen communication) to engage in democratic deliberations, e-activism and e-campaigning, put forward their concerns, ideas and initiatives, promote dialogue and deliberation with representatives and government, and to scrutinise officials and politicians in matters of public interest.

Privacy and data protection

65. The right to respect for family and private life is enshrined in Article 8 of the ECHR. This right is further interpreted by the case-law of the Court and complemented and reinforced by the Council of Europe Convention 108.

66. Private life is a notion not susceptible to exhaustive definition. The Court has emphasised that Article 8 encompasses a wide range of interests, namely private and family life, home, and correspondence including mail, telephone communications[55] and e-mails in the workplace. Private life relates to a person's right to their image[56], for example by means of photographs and video-clips. It also concerns a person's identity and personal development, the right to establish and develop relationships with other human beings. Activities of a professional or business nature are also covered.[57]

67. Many activities of users will involve some form of automatic processing of personal data; examples include the use of browsers, e-mail, instant messages, voice-over Internet protocols, social networks and search engines as well as cloud data storage services. Convention 108 covers all operations carried out in the Internet, such as collection, storage, alteration, erasure and retrieval or dissemination or personal data. [58]

68. There are principles and rules that should be respected by public authorities and private companies which are engaged in the processing of personal data. It is necessary that a user is aware of and understands what and how her/his data is processed and whether action can be taken in this regard, for example to request correction or erasure of data. According to Convention 108, personal data must be obtained and processed fairly and lawfully, and stored for specified and legitimate purposes. It must be 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 person whose personal data are processed and for no longer than is required for the purpose for which those data are stored.[59]

69. Emphasis is placed on two specific principles of the processing of personal data: the lawfulness of the processing, and the user's consent. The user must be informed that data can be processed only when this is laid down by law and when she/he has consented to it, for example by agreeing to the terms and conditions of use of an Internet service.

[54] See note 9 above, CM/Rec(2007)16, Appendix, part I.
[55] Klass and Others v. Germany, no 5029/71, §41.
[56] Von Hannover v. Germany (no. 2), nos. 40660/08 and 60641/08 §§ 108-113.Sciacca v. Italy, no. 50774/99, § 29.
[57] 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).
[58] See Convention 108, Article 2.
[59] Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (ETS No.108).

70. A person's free, specific, informed and explicit (unambiguous) consent to the processing of personal data on the Internet is currently being discussed to be integrated in the Convention 108.[60] Informed consent is referred to in the 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. In particular, social networks should secure the informed consent of their users before their personal data is disseminated or shared with other categories of people or companies or used in ways other than those necessary for the specified purposes for which they were originally collected. In order to ensure users' consent, they should be able to "opt in" to a wider access to their personal data by third parties (e.g. when third party applications are operated on the social network). Equally, users should also be able to withdraw their consent.

71. It is important to note 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. This is understood as automatic data processing techniques that consist of applying a profile to an individual in order to take decisions concerning him or her or for purposes of analysing or predicting his or her personal preferences, behaviours and attitudes. For 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. by collecting information on pages and content visited, times of visits, what was searched for, what was clicked). 'Cookies' are one of the means used to track users' browsing activities; this is done by storing information in a user's equipment retrieving it later on. The Recommendation envisages the right of Internet users to consent to the use of personal data for the purposes of profiling and the right to withdraw such consent.[61]

72. Internet users' rights to information with regard to the processing of his/her personal data are referred to in different Council of Europe instruments. Convention 108 provides that the data subject should be enabled to establish the existence of processing of his/her personal data by any natural or legal person, the main purposes of the processing as well as the identity and habitual residence or principal place of business of the processing entity and 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. [62]

73. Information to users is also referred to in 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. Internet users on social networks should be informed in a clear and understandable manner about every change made to the providers' terms of service and conditions of use. This also includes other actions, such as the installation of third party applications which involve risks to users' privacy; the law that is applicable in the execution of the social networking services and the related processing of their personal data; the consequences of open access (in time and geographically) to their profiles and communications, in particular explaining the differences between private and public communication, and the consequences of making information publicly available, including unrestricted access to, and collection of, data by third parties; and- the need to obtain the prior consent of other people before they publish their personal data, including audio and video content, in cases where they have widened access beyond self-selected contacts. Internet users should also be given specific information regarding the logic underpinning the processing of personal data that is used to attribute a profile to him/her and the purposes of profiling.

74. Internet users should be able to exercise control over their personal data as developed in Convention 108, notably the right to obtain rectification or erasure of data that has been processed contrary to the law and the right to 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.[63]

[60] The Consultative Committee of the Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (ETS No.108) has made a number of proposals to modernise this convention (T-PD(2012)4Rev3_en). One of the proposals focuses on the consent of the person whose personal data are processed as a pre-condition for such processing "Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and [explicit, unambiguous] consent of the data subject or of some legitimate basis laid down by law."

[61] 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.

[62] Convention 108, Article 8.

[63] See note 60 above, Article 8.

75. The Committee of Ministers Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, refers to a number of measures that providers can take to protect their users' privacy. This includes the protection of personal data against unlawful access by third parties and data breach notification schemes. Measures should also include "end-to-end" encryption of the communication between the user and the search engine provider. Cross-correlation of data originating from different services/platforms belonging to a search engine provider can take place only if unambiguous consent has been granted by the user for that specific service. Users should be able to access, correct and delete their data that is collected in the course of the use of such services, including any profile created, for example for direct marketing purposes.[64]

76. Social networks should also assist users in the management and protection of their data in particular with:

- *default privacy-friendly settings,* to limit access to contacts identified and selected by the user. This includes adjustments to their privacy settings and to the selection of the level of public access to their data;

- *enhanced protection for sensitive data,* such as biometric data or facial recognition access which should not be activated by default;

- *data security against unlawful access to user's personal data,* by third parties, including end-to-end encryption of communication between the user and social networks. Users should be informed about breaches of their personal data security in order to be able to take preventive measures such as changing their passwords and being attentive to their financial transactions (for example when social networks are in possession of bank or credit card details);

- *privacy by design,* that is addressing data protection needs at the stage of conception of their services or products, and continuously assessing the privacy impact of changes to existing services;

- *protection for non-users of social networks* by refraining from collecting and processing their personal data, for example e-mail addresses and biometric data. Users should be made aware of the obligations they have towards other individuals and, in particular, that the publication of personal data related to other people should respect the rights of those individuals.[65]

77. Before a social network user's account is terminated, he/she should be able to easily and freely move his/her data to another service or device, in a usable format. Upon termination, all data from and about the user should be permanently eliminated from the storage media of the social networking service. In addition, Internet users should be able to make informed choices about their online identity, including the use of a pseudonym. In the event that a social networking service requires real identity registration, the publication of that real identity on the Internet should be optional for users. This does not prevent law-enforcement authorities from gaining access to the user's real identity when necessary and subject to appropriate legal safeguards guaranteeing the respect of fundamental rights and freedoms.

78. In the context of profiling, the user should also be able to object to the use of his/her personal data for the purpose of profiling and to object to a decision taken on the sole basis of profiling, which has legal effects concerning him/her or significantly affects him/her, unless this is provided by law which lays down measures to safeguard the users' legitimate interests, particularly by allowing him/her to put forward his point of view and unless the decision was taken in the course of the performance of a contract and provided that the measures for safeguarding the legitimate interests of the Internet user are in place. [66]

[64] See CM/Rec(2012)3, in particular Appendix, part II.
[65] Ibid.
[66] 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.

79. The rights of the Internet user are not absolute hence the reference to the word 'generally' in the third sub-paragraph. Derogations are permissible when this is provided for by law and it constitutes a necessary measure in a democratic society in the interests of: (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; and (b) protecting the data subject or the rights and freedoms of others. Restrictions on the exercise of the rights foreseen 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.[67]

80. Interception relates to the listening to, monitoring or surveillance of content of communications, securing the content of data through the access and use of the computer system, or indirectly through the use of electronic eavesdropping or tapping devices. Interception may also involve recording.[68] The right to respect for the confidentiality of correspondence and communications is enshrined in Article 8 of the ECHR, which has been further interpreted by the Court. The concept of correspondence covers mail and telecommunications[69] as well as e-mails sent in a working context[70]. It is expected that the interpretation of this concept will evolve to keep pace with the developments of technology which may bring other forms of communications on the Internet, such as email messages (in a broader context), instant messaging or others within the sphere of Article 8 protection.

81. Some of the general principles affirmed in the Court case-law with regard to interception and surveillance of communications in non-Internet cases and cases involving interferences by State authorities are given below. These principles provide general guidance and reference, for possible future application to Internet communications.

82. The interception of correspondence and telecommunications are interferences with the right to private life and subject to the conditions of Article 8 paragraph 2 of the ECHR. The very existence of legislation permitting surveillance of telecommunications may be considered as an interference with the right to private life. A law that institutes a system of surveillance, under which all persons in the country concerned can potentially have their mail and telecommunications monitored, directly affects all users or potential users of the postal and telecommunication services in that country. The Court has, therefore, accepted that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them, without having to allege that such measures were in fact applied to him or her.[71]

83. Interception must have a basis in law and be necessary in a democratic society in the interest of the 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, as foreseen in Article 8 of the ECHR. The Court has developed the following general principles with particular reference to the requirements that the law, providing for covert measures of surveillance of correspondence and communications by public authorities, should meet.

- *Foreseeability* – the law must be accessible to the person concerned who must be able to foresee the consequences of its application to him/her. The law must also be formulated with sufficient clarity and precision to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.[72]

[67] Convention 108, Article 9.
[68] See Explanatory Report to the Budapest Convention, para.53.
[69] Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria no. 62540/00 § 58; Klass and Others v. Germany no 5029/71, Malone v. the United Kingdom, no 8691/79 and Weber and Saravia v. Germany, no 54934/00.
[70] See Copland v. UK, no 62617/00.
[71] Klass and Others, no 5029/71 §§ 30-38; Malone v. the United Kingdom no 8691/79§ 64; and Weber and Saravia v. Germany no. 54934/00, §§ 78 and 79, Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria no. 62540/00 § 58, § 69-70.
[72] Malone v. the United Kingdom, no 8691/79 § 67; Valenzuela Contreras v. Spain, judgment of 30 July 1998, Reports 1998-V, p. 1925, § 46 (iii); and Khan v. the United Kingdom, no.35394/97, § 26, Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria, no. 62540/00, §71.

- *Minimum safeguards for the exercise of discretion by public authorities* – the law should have detailed rules on (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 (v) 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.[73]

- *Supervision and review by competent authorities* – the Court requires that there exist adequate and effective guarantees against abuse.[74]

84. Court's case law on privacy in the workplace has found that telephone calls made by an employee in the premises of the enterprise are covered by the notions of private life and correspondence. Emails sent from work as well as information derived from the monitoring of personal Internet usage should be protected under Article 8 of the ECHR. In the absence of a warning that these would be liable to monitoring, the employee has a reasonable expectation that her/his privacy is respected with regard to phone calls, email and Internet usage in the workplace.[75] The user can be assisted by data protection authorities, or other competent authorities in member States.

85. Data protection authorities, existing in a vast majority of member States, play an important role in investigating, intervening, raising awareness or otherwise remedying interferences in the processing of personal data. This is notwithstanding the primary role of the State to assure the protection of personal data within the wider scope of their obligation to safeguard the right to private and family life.

Education and literacy

86. The right to education is enshrined in Article 2 of Protocol 1 to the ECHR. The Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet encourages the creation and processing of and 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.[76] Internet users should be able to freely access publicly funded research and cultural works on the Internet. [77] Access to digital heritage materials, which are in the public domain, should also be freely accessible within reasonable restrictions. Conditions on access to knowledge are permitted in specific cases in order to remunerate right holders for their work, within the limits of permissible exceptions to intellectual property protection.

87. Internet users should have the ability to acquire basic information, education, knowledge and skills in order to exercise their human rights and fundamental freedoms on the Internet. This is in line with the Council of Europe's Committee of Ministers standards which promote computer literacy as a fundamental prerequisite for access to information, the exercise of cultural rights and the right to education through ICTs.[78]

88. Internet literacy programmes and initiatives enable Internet users to critically analyse the accuracy and trustworthiness of Internet content. The Committee of Ministers has recommended that Council of Europe Member States should facilitate access to ICT devices and promote education to allow all persons, in particular children, to acquire the skills needed to work with a broad range of ICTs and assess critically the quality of information, in particular that which could be harmful to them.[79]

[73] See Kruslin v France, no. 11801/85 § 33; Huvig v. France, no 11105/84 § 32; Amann v. Switzerland, no27798/95 § 56; Weber and Saravia v. Germany, no 54934/00§ 93; Association for European Integration and Human Rights and Ekmidzhiev v. Bulgaria, no. 62540/00 § 76.
[74] Ibid., no. 62540/00) § 77.
[75] Copland v. UK, no 62617/00, §41, 42.
[76] See also note 8 above, CM/Rec(2007)16 Section IV.
[77] Ibid.
[78] Committee of Ministers Declaration on human rights and the rule of law in the Information Society, CM(2005)56 final 13 May 2005.
[79] Ibid.

Children and young people

89. Children and young person have the right to express their views, to participate in society as well as in the decisions affecting them by means of the Internet and other ICTs. This is based on Committee of Ministers standards which state that all children and young people under the age of 18 should have the right, the means, the space, the opportunity and, where necessary, the support to freely express their views, to be heard and to contribute to decision making on matters affecting them, their views being given due weight in accordance with their age, maturity and understanding. The right of the child and young people to participate applies fully to Internet environments without any discrimination on any grounds such as race, ethnicity, colour, sex, language, religion, political or other opinion, national or social origin, property, disability, birth, sexual orientation or other status.[80]

90. Children and young people should be provided with information appropriate to their age and circumstances, including through social networking and other media, on the opportunities available to them to exercise their rights. They should be fully informed about the scope of their participation, including limitations of their involvement, the expected and actual outcomes of their participation and how their views were ultimately considered.[81] Where they consider their right to participate has been violated they should be provided with effective redress and remedies, such as child-friendly means of making complaints and judicial and administrative procedures including assistance and support in using them.[82]

91. Children and young users should be able to use the Internet in safety and with due regard for their privacy. They should receive training and information from teachers, educators and parents. Their information literacy is understood as meaning the competent use of tools providing access to information, the development of critical analysis of content and the appropriation of communication skills to foster citizenship and creativity, as well as training initiatives for children and their educators in order for them to use the Internet and information and communication technologies in a positive and responsible manner.[83]

92. Children's right to private life has been the object of examination in cases brought before the Court. The physical and moral welfare of children are essential aspects of their right to private life. Member States have positive obligations to ensure effective respect for this right.[84] The Court considers that effective deterrence against grave acts where fundamental values and essential aspects of private life are at stake, requires efficient criminal law provisions and investigations.[85]

93. It is important to understand that the content that children and young people create on or using the Internet or content others create in relation to them (e.g. pictures, videos, text or other content) or the traces of this content (logs, records and processing) may last or be permanently accessible. This may challenge their dignity, security and privacy or otherwise render them vulnerable now or at a later stage in their lives. They themselves, as well as their parents, guardians, teachers and carers, should be empowered to understand and cope with this reality as well as to protect their privacy online. To this end, it is important that practical advice is made available on how to have personal information erased. The Council of Europe's Committee of Ministers has provided guidance to its member States, by stating 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. [86] Therefore, member States were invited together, where appropriate, with other relevant stakeholders, to explore the feasibility of removing or deleting such content, including its

[80] Recommendation CM/Rec(2012)2 of the Committee of Ministers to member States on the participation of children and young people under the age of 18.
[81] Ibid.
[82] See Recommendation CM Rec(2011)12 of the Committee of Ministers to member States on children's rights and social services friendly to children and families, Council of Europe Guidelines on Child-Friendly Justice.
[83] Recommendation Rec(2006)12 of the Committee of Ministers on empowering children in the new information and communications environment.
[84] K.U. v. Finland - 2872/02 § 40, 41.
[85] X and Y v. the Netherlands, §§ 23-24 and 27; August v. the United Kingdom no. 36505/02; and M.C. v. Bulgaria, no. 39272/98, § 150. K.U. v. Finland, no 2872/02 § 46.
[86] Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet.

traces (logs, records and processing), within a reasonably short period of time.[87] Sub-paragraph 3, however, does not apply to content regarding children or young people created by the press or publishers. The first sentence in this provision of the Guide specifies that it addresses situations relating to content created by children or young people or other Internet users about them.

94. As regards harmful content and behaviour online, children are entitled to special care and assistance that is appropriate to their age and circumstances, in particular with regard to the risk of harm which may arise from online pornography, the degrading and stereotyped portrayal of women, the portrayal and glorification of violence and self-harm, in particular suicides, demeaning, discriminatory or racist expressions or apologia for such conduct, solicitation for sexual abuse purposes, 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.[88] Children and young Internet users should therefore be informed, in a way that is adapted to their age and any other particular circumstances, about the types of content and behaviour that are illegal.

95. Children and young people should also be able to report content and behaviour which poses a risk of harm, and to receive advice and support, with due regard to their confidentiality and anonymity. This is particularly relevant in the context of social networks. The Committee of Ministers has recommended to its member States to take action in this respect[89] in particular to protect children and young people from harmful content by:

- providing clear information about the kinds of content or content-sharing or conduct that may be contrary to applicable legal provisions;

- developing editorial policies so that relevant content or behaviour can be defined as "inappropriate" in the terms and conditions of use of the social networking service, while ensuring that this approach does not restrict the right to freedom of expression and information;

- setting up easily accessible mechanisms for reporting inappropriate or apparently illegal content or behaviour posted on social networks;

- providing due-diligence response to complaints of cyber-bullying and cyber-grooming. [90]

96. Children and young users should also be informed about the risks of interference with their physical and moral welfare, including sexual exploitation and abuse in online environments which necessitates special protection. This is referred to in the Council of Europe's Lanzarote Convention, and in the relevant case law of the Court which recognises that States have positive obligations to ensure the protection of children online.[91]

97. According to the Lanzarote Convention, children should be protected from being recruited, caused or coerced into participating in pornographic performances made accessible or available on the Internet (for example through webcams, in chat rooms or online games).[92] They must also be protected from solicitation through the use of the Internet or other ICTs 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.[93]

[87] Ibid.
[88] 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.
[89] See CM/Rec(2012)4 , Appendix, II, §10.
[90] Ibid.
[91] K.U. v. Finland no. 2872/02.
[92] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No.: 201, Article. 2; Article 21, see also Explanatory Report on these articles.
[93] Ibid. Article 23.

98. Children should be encouraged to participate in the development and implementation of State policies, programmes or others initiatives concerning the fight against sexual exploitation and sexual abuse of children in Internet environments.[94] They should be provided with child-friendly and accessible means of reporting alleged sexual abuse and exploitation on the Internet and making complaints through information services such as telephone and Internet helplines. They should be provided with advice and support in using these services with due regard to their confidentiality and anonymity.[95]

Effective remedies

99. The right to an effective remedy is enshrined in Article 13 of the ECHR. Everyone whose rights and freedoms are restricted or violated on the Internet has the right to an effective remedy.

100. Article 13 of the ECHR guarantees the availability, at the national level, of a remedy to enforce the substance of ECHR rights and freedoms in whatever form they might happen to be secured in the domestic legal order. It requires the provision of a domestic remedy to deal with the substance of a complaint under the ECHR and to grant appropriate relief.[96] States have a positive obligation to carry out an investigation of allegations of human rights infringement that is diligent, thorough and effective. The procedures followed must enable the competent body to decide on the merits of the complaint of violation of the Convention and to sanction any violation found but also to guarantee the execution of decisions taken.[97]

101. There should be a national authority tasked with deciding on allegations of violations of the rights guaranteed in the ECHR.[98] There must be a specific legal avenue available whereby an individual can complain about the unreasonable length of proceedings in the determination of his/her rights.[99] The authority may not necessarily be a judicial authority if it presents guarantees of independence and impartiality. However, its powers and the procedural guarantees afforded should permit a determination whether a particular remedy is effective.[100]

102. The procedure followed by the competent national authority should permit effective investigation of a violation. It should allow the competent authority to decide on the merits of the complaint of a violation of ECHR rights,[101] to sanction any violation and to guarantee the victim that the decision taken will be executed.[102] The remedy must be effective in practice and in law and not conditional upon the certainty of a favourable outcome for the complainant.[103] Although no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided in law may do so. [104]

103. Effective remedies should be available, known, accessible, affordable and capable of providing appropriate redress. Effective remedies can also be obtained directly from Internet service providers (although they may not enjoy sufficient independence to be compatible with Article 13 ECHR), public authorities and/or other national human rights institutions. Possibilities for redress include an inquiry, an explanation by the service provider or online provider, the possibility to reply to a statement which is considered for example defamatory or offensive, reinstatement of user-created content that has been removed by an online service provider, and reconnection to the Internet when Internet users have been disconnected and related compensation.

---

[94] Ibid. Article 9/1.
[95] Ibid. Article 13. See also Recommendation CM/Rec(2011)12 of the Committee of Ministers to member States on children's rights and social services friendly to children and families, Council of Europe Guidelines on Child-Friendly Justice.
[96] Kaya v. Turkey, no. 22729/93, §106.
[97] Smith and Grady v. UK, no 33985/96 33986/96.
[98] Silver and Others v. UK, no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 §113; Kaya v. Turkey, no. 22729/93, §106.
[99] Kudla v. Poland, no. 30210/96, §157.
[100] Silver and Others v. UK, no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 §113; Kaya v. Turkey, no. 22729/93, §106.
[101] Smith and Grady v. UK, no 33985/96 33986/96, § 138.
[102] Iatridis v. Greece, no. 31107/96, § 60.
[103] Kudla v. Poland, no. 30210/96, §158.
[104] Silver and others v. UK, no.5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 §113; Kudla v. Poland, no. 30210/96 §157.

104. States, as part of their positive obligations to protect individuals against violations of human rights by private companies, should take appropriate steps to ensure that when such violations occur those affected have access to judicial and non-judicial mechanisms.[105] The United Nations Guiding Principles on Business and Human Rights specify that companies should establish complaint mechanisms which are accessible, predictable (providing clear and known procedure with indication of time frames for each stage of the process, clarity on the types of process and outcomes available and the means for monitoring their implementation) equitable (access to sources of information, advice and expertise), transparent and capable to offer remedies which are in full compliance with international human rights standards directly to individuals.[106]

105. Internet users should be offered clear and transparent information regarding the means of redress available to them. This information could be included in terms of use and/or service or in other guidelines and policies of Internet service/online providers. Internet users should be provided with practical and accessible tools to contact Internet service/online providers to report their concerns. They should be able to request information and seek remediation. Some examples of remedies which may be available to Internet users are helplines or hotlines run by Internet service providers or consumer protection associations to which Internet users can turn in the case of violation of their rights or the human rights of others. Guidance should be provided by public authorities and/or other national human rights institutions (ombudspersons), data protection authorities, regulators for electronic communications, citizens' advice offices, human rights or digital rights associations or consumer organisations.

106. Internet users should be protected from cybercrime. States who are signatory parties to the Budapest Convention have undertaken obligations to protect citizens from criminal activities and offences on the Internet. Internet users have a reasonable expectation to be protected from criminal activity or criminal offences committed on or using the Internet.

107. The focus is on offences against confidentiality and integrity of computer data and systems and computer-related offences. Content-related offences (child pornography, copyright infringement) are not covered here as these are considered to be dealt with in the parts of the Guide relating to the rights of the child. The protection of right-holders is considered to implicate the interests of this particular group rather than those of Internet users. Also, interceptions and surveillance of communications are dealt with in the section on privacy and data protection.

108. Internet users have a legitimate interest to manage, operate and control their computer systems in an undisturbed and uninhibited manner. They should be protected from illegal access to the whole or parts of computer systems used by them including hardware, components, stored data of the system installed, directories, traffic and content-related data. This also includes protection from unauthorised intrusion into computer systems and data (hacking, cracking or other forms of computer trespass) which may lead to impediments to Internet users of systems and data such as access to confidential data (passwords, information and secrets etc).[107]

109. Internet users should also be protected against computer data interference, such as malicious code (for example viruses and Trojan horses).[108] They should also be protected against interference with the functioning of computer or telecommunication systems by inputting, transmitting, damaging deleting, altering or suppressing computer data[109] as for example programmes that generate 'denial of service attacks, malicious codes such as viruses that prevent or substantially slow down the operation of the system, or programmes that send large quantities of electronic mail to a recipient in order to block communication functions of the system (spamming). This may be an administrative or criminal offence depending on domestic legislation.

[105] The issue of corporate social responsibility and States positive obligations to protect human rights are explained in paragraphs19 and 28 of the Explanatory Memorandum.
[106] See Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (A/HRC/17/31) endorsed by the Human Rights Council by Resolution Human rights and transnational corporations and other business enterprises A/HRC/RES/17/4, chapter III, principles 28-31.
[107] Budapest Convention on Cybercrime, Article 2, Explanatory Report, §.44-50.
[108] Ibid. Article 4, Explanatory Report §, 60-61.
[109] Ibid. Article 5, Explanatory Report § 65-69.

110. Internet users should be protected against computer forgery which involves unauthorised creation or alteration of data so that they acquire a different evidentiary value in the course of legal transactions, which rely on the authenticity of information contained in the data.[110]

111. Internet users have a legitimate interest in the protection of assets represented or administered in computer systems (electronic funds, deposit money). They should be protected against computer fraud manipulations which produce a direct economic or possessory loss of an Internet user's property (money, tangible and intangibles with an economic value) such as credit card fraud.[111]

112. Any security measure aimed at ensuring the protection of Internet users from cyber-crime must be in full compliance with the standards of the ECHR, in particular the right to private and family life and the right to freedom of expression.[112]

113. Internet users have the right to fair trial, which is enshrined in Article 6 of the ECHR. This refers to the determination of civil rights and obligations or criminal charges with regard to activities of Internet users. In particular, this concerns key principles pronounced by the Court, namely the right to a fair and public hearing within a reasonable time by an independent and impartial court; the right to institute proceedings before courts, to a final determination of the dispute, to a reasoned judgment and to the execution of the judgment; the right to adversarial proceedings and equality of arms and others.

114. The Court, although not in Internet-related cases, has established general principles with regard to the quality of administration of justice (independence, impartiality, competence of the tribunal), the protection of right of the parties (fair hearing, equality of arms and public hearing) as well as with regard to the efficiency of justice administration (reasonable time).

115. The Internet user has the right to file an individual application to the Court after exhausting all domestic remedies that are available and effective, within six months[113] from the date on which a final decision was taken.

[110] Ibid. Article 7, Explanatory Report § 81.
[111] Ibid. Article 8, Explanatory Report § 86-88.
[112] Ibid. Article 15.
[113] This deadline will be four months once Protocol No. 15 to the ECHR has entered into force.

PREMS 703114

GBR

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It includes 47 member states, 28 of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE