Committee of experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

MSI-INT (2015)06rev
19 October 2015

Draft Explanatory memorandum to the draft Recommendation CM/Rec__ (2015) ___of the Committee of Ministers to member States on Internet Freedom

Background and the process

1. The Ministers of States participating in the Council of Europe Conference of Ministers responsible for media and information society, held in Belgrade, Serbia, on 7 and 8 November 2013 adopted a Resolution on Internet freedom. The Resolution invited the Council of Europe to further develop, in a multi-stakeholder approach, the notion of "Internet freedom" on the basis of standards adopted by the Committee of Ministers on Internet governance principles, network neutrality and the universality, integrity and openness of the Internet".

2. The Committee of Ministers approved the terms of reference of the Committee of experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT) at its 1185th meeting, 20 November 2013 (CM(2013)131 add final). Under its terms of reference the MSI-INT is expected to prepare and submit to the CDMSI a draft recommendation on Internet freedom. Subsequently the Committee of Ministers Decisions of the Committee of Ministers adopted at the 1187th meeting, 11-12 December 2013 instructed the Steering Committee on Media and Information Society (CDMSI) "to develop, in a multi-stakeholder approach, the notion of "Internet freedom" on the basis of standards adopted by the Committee of Ministers on Internet governance principles, network neutrality and the universality, integrity and openness of the Internet".

3. The MSI-INT held its first meeting on 17 and 18 March 2014, in Strasbourg. While noting the potential broad nature of the notion of Internet freedom, the MSI-INT agreed to focus its reflections on defining the notion and exploring it further in discussions with stakeholders as appropriate in the European Dialogue on Internet Governance (EuroDIG, 12-13 June 2014, Berlin) and the Internet Governance Forum (IGF, 2-5 September 2014, Istanbul).

4. Discussions at the second meeting the MSI-INT, which took place on 3 and 4 July 2014 in Strasbourg, highlighted that the added value of this instrument would be to recommend that member states consider Internet freedom in a comprehensive manner. The draft recommendation could be envisaged as a tool to guide policy-makers and to help member states evaluate the state of Internet Freedom as well as

structure the debate internationally regarding Internet freedom. The MSI-INT agreed on a preliminary draft recommendation which aims at encouraging member State to implement human rights standards online and includes a list of indicators on Internet freedom.

5. At its working meeting, which took place on 23 and 24 October 2014 in Strasbourg, the MSI-INT validated the general approach taken in the draft recommendation as regards periodical reviews of the state of Internet freedom at a national level on the basis of the indicators set out in the draft recommendation. The objective is to promote an enabling environment in Council of Europe member states for the exercise and enjoyment of fundamental rights and freedoms online. The Internet freedom indicators should be geared towards facilitating an effective implementation of human rights standards. Participants from the private sector considered that the draft recommendation would be able to give guidance to civil society and citizens to strengthen their observatory role on Internet freedom. The CDMSI at its 7th meeting (18-21 November 2014) took note of the preliminary draft recommendation and invited its members to send possible comments to the MSI-INT.

6. At its third meeting, which took place on 5 and 6 March 2015 in Strasbourg, the MSI-INT discussed extensively the preamble and the operative parts of the draft recommendation. Pursuant to the Committee of Ministers Decision to develop in a multi-stakeholder approach the notion of Internet freedom, the MSI-INT agreed to organise multi-stakeholder consultations until the end of April 2015. Therefore, the MSI-INT agreed to propose to the Bureau of the CDMSI that the Steering Committee on Human Rights Policy (CDDH), the Steering Committee on Crime Problems (CDPC), the European Committee on Legal Cooperation, the Consultative Committee of the Data Protection Convention (T-PD) and the Cybercrime Convention Committee (T-CY) be invited to provide their comments. In addition, the draft recommendation should be uploaded on the website of the Council of Europe and stakeholders be invited to comment.

7. Further to approval by the Bureau of the CDMSI of the MSI-INT proposals multi-stakeholder consultations were organised during the period of time 30 April – 14 May 2015. Comments were offered by members of the CDDH, CDCJ and the T-PD Bureau and TC-Y. 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 recommendation and provided numerous comments and proposals for changes thereto.

8. The CDMSI, at its 8th meeting (16-19 June 2015), took note of the comments provided during the multi-stakeholder consultations. It supported the overall strategic approach of the draft recommendation to promote implementation of existing human rights standards on the Internet. It agreed to invite delegations to provide comments to the MSI-INT by 31 July 2015.

9. The MSI-INT, at its last meeting (7-8 September 2015, Strasbourg), finalised its proposals to the CDMSI for a draft recommendation by the Committee of Ministers CM/Rec(2015)__ to the member States on Internet freedom.

[10. The CDMSI at its 9th meeting (8-11 December 2015, Strasbourg) finalised a draft recommendation by the Committee of Ministers CM/Rec(2015)__ to the member States on Internet freedom and agreed to transmit it to the Committee of Ministers for possible adoption.]

Commentary on Recommendation CM/Rec (2014)___ of the Committee of Ministers to member States on Internet freedom

Preamble of the Recommendation

11. The preamble affirms the principle that human rights and fundamental freedoms apply both to offline and online environments. The key standard is the ECHR. The central idea of the preamble is that Internet freedom should not be considered as a matter of choice with regard to which rights and freedoms should be protected. Instead a comprehensive approach with regard to all indicators should be taken.

12. Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms. States are the duty bearers with regard to the protection and promotion of human rights in compliance with the ECHR. The role and the participation of States in Internet governance arrangements is considered as one of the conditions for the realisation of human rights and fundamental freedoms. Hence, the recommendation makes reference in paragraph 3 to the role and responsibilities of States with regard to international Internet-related policy. This paragraph is based on the Declaration of Committee of Ministers on Internet governance principles adopted in 2011.

13. The recommendation is based on the premise that in order for Internet freedom to exist it is necessary that legal, economic and political conditions are in place. It is the role of States to evaluate whether such conditions exist. Consequently it is recommended that member States evaluate the Internet freedom landscape using the indicators identified on the basis of existing Council of Europe standards. These evaluations will help member States to evaluate the state of play with regard to the implementation of standards and will provide an impetus for better and more effective implementation whenever this is necessary. The ECHR and other Council of Europe standards provide benchmarks and references for national evaluations of Internet freedom. Therefore, they can be conceptualised as indicators of Internet freedom.

14. In the operative part of the recommendation the Committee of Ministers recommends to member States to periodically evaluate how human rights standards are implemented and respected. Member States are better placed to assess the frequency or periodicity of self-assessment and preparation of Internet freedom report, based on their appreciation of their institutional capacities to prepare such reports. Also, it is left to the appreciation of member States whether or not they share national reports on Internet freedom with the Council of Europe. These reports can be considered as part of the reflection by the Secretary General in the preparation of his annual report on the state of democracy, human rights and rule of law in Europe. The objective is to promote the implementation of existing standards and the sharing of best practices.

Internet Freedom Indicators

15. The indicators included in the Recommendation are intended to provide guidance in conducting a qualitative and objective evaluation of and reporting on the enabling environment for Internet freedom in Council of Europe member states. The explanatory memorandum provides complementary information on their basis in international human rights standards. In addition, it suggests sources of verification wherever applicable to the indicators, which can be used by national authorities when completing national evaluations.

1. An enabling environment for Internet freedom

16. A key principle of the Council of Europe's Internet-related standards, that is fundamental rights and freedoms apply both to online and offline environments[1]. The European Court of Human Rights (ECtHR) has affirmed that "the 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." [2] The ECtHR has underscored that the Internet is an important medium where citizens exercise their fundamental rights and that ECHR rights apply to the Internet[3]. The UN Special Rapporteur on freedom of expression stated that the Internet acts 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".[4]

17. *Indicator 1.1.* seeks to verify that the State has enshrined these principles in its legal system. This could be done in constitutional or other laws, addressing the issue of human rights protection. These would be the sources of verification in evaluations based on this indicator. This indicator does not require that constitutional or other laws specifically mention their application to the Internet. It is important that their application is not limited to the physical world only, thus excluding the implementation of human rights standards with regard to the Internet. Another form of verification could be any international human rights treaties accepted by member States with no significant exemptions or any other integration of international human rights standards in legislation or policy related to the Internet.

18. Member States should assess the compliance of their actions which interfere with the right to private life, the right to freedom of expression, and the right to freedom of assembly and association with Articles 8, 10 and 11 of the ECHR. Sources of verification of *Indicator 1.2.* are laws and policies that restrict these rights and freedoms. These should be in compliance with the requirements of the ECHR as interpreted by the ECtHR: any restrictions pursue one of the legitimate aims foreseen in the ECHR and are necessary and proportionate in a democratic society. The least restrictive means should be used to achieve the legitimate aim.

---

[1] See Committee of Ministers Declaration on Internet Governance Principles, principle 1 "Human Rights, Democracy and Rule of Law"
[2] EctHR Application no. 3111/10 Yildirim v Turkey, Judgment, Final 18.03.2013 Paragraph 54
[3] Neij and Sunde Kolmisoppi v. Sweden no.40397/12, Decision 19 February 2013 , p9
[4] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations General Assembly 16 May 2011, p.22.

19. Further verification will be that States ensure that private actors are able to provide the guarantees for these rights and freedoms, where those actors are operating infrastructure or facilities necessary for their exercise. The United Nations Guiding Principles on Business and Human Rights provide additional guidance[5]. The ECtHR has held States accountable for failing to protect their citizens from adverse effects on their rights and freedoms resulting from actions of private companies.[6]

20. Regulation of Internet issues is often distributed in different legal or policy instruments. Hence it is necessary not only to coordinate their preparation for coherence but also to asses the negative impact they could have on the exercise and enjoyment of human rights and fundamental freedoms. In addition, such approach will enable States to establish a careful balance of the competing rights. *Indicator 1.3.* asks States to assess how any such laws and policies restricting these rights and freedoms have been balanced against other rights and freedoms being protected and that the appropriate legal tests are conducted.

21. States also have a duty to ensure the foreseeability of any laws and policies that they put in place in compliance with the requirements and principles established by the ECtHR in interpretation of the ECHR. An element of foreseeability is that laws and policies are assessed for compliance with ECHR before they are adopted, and that such compliance requirement is fully respected by the State. Any report, supporting explanatory statement on draft legislation or policy can serve as a source of verification.

22. *Indicator 1.4.* is based on the principle of multi-stakeholder governance included in the Committee of Ministers Declaration on Internet Governance principles. It builds on the definition of Internet governance, this principle affirms the multi-stakeholder nature of Internet environments. It reflects the understanding of the Geneva Declaration of Principles which states that "[g]overnments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires co-operation and partnership among all stakeholders." It also underlines that "[t]he international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations".

23. The requirement of foreseeability of laws means that individual citizens must be able to foresee the consequences of its application to him/her and 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 act. An open process of lawmaking will assist with the foreseeability requirement.

---

[5] Report of the Special Representative of the Secretary- General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, 21 March 2011

[6] Lòpez 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.

24. As a means of verification of this indicator, use can be made of any information, such as reports, articles or otherwise, on activities undertaken by competent State authorities to consult with stakeholders. These activities can include, conferences, meetings, seminars, public fora, consultations on draft laws and policies or any other form of engagement of public officials in public debates around Internet related policy issues.

25. *Indicator 1.5.* requires wherever the law provides that executive authorities or regulatory bodies have discretion to implement measures which restrict the exercise or enjoyment of fundamental rights and freedoms, the law provides sufficient safeguards for the autonomy and independence from political or commercial interests. The members of regulatory bodies should be chosen through a democratic and transparent process in order to minimize partisan or commercial interference. Their powers and responsibilities should be set out in law, including explicit requirements to promote freedom of expression, the free flow of information, privacy and freedom of assembly and association. Any law or other legal instrument on the role membership, and competencies of regulatory bodies can serve as means of verification of this indicator.

26. Internet users and individuals in general should be protected from cybercrime. This will create a secure environment in which all will feel safe to exercise their rights and freedoms, hence contributing to the overall environment for Internet freedom. *Indicator 1.6.* can be verified by any law or policy which criminalises offences against the confidentiality and integrity of computer data and systems; content related offences (child pornography, copyright infringement); illegal access to the whole or parts of computer systems (hardware, components, stored data etc);intrusion into computer systems (hacking, cracking or other forms of computer tress pass) which may lead to access to confidential data; computer data interference, such as malicious code (for example viruses and Trojan horses); interference with the functioning of computer or telecommunication systems by inputting, transmitting, damaging deleting, altering or suppressing computer data 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); computer forgery etc. All measures taken to combat cybercrime should comply with the articles 8, 10 and 11 of the ECHR.

27. Since Internet companies are the main interlocutor or the party with which individuals have contacts with regard to the exercise of the human rights and freedoms on the Internet their responsibilities to protect, respect and remedy these rights are key to the creation of an enabling environment for Internet freedom to exist and develop. Therefore, *Indicator 1.7.* refers to the United Nations Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. 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.[7]

28. A foundational principle of the Guiding Principles on Business and Human Rights 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.

29. 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. [8]

30. Verification of Indicator 1.7. can be sought in any law and policy which implements the Guiding Principles explained above or any other action plan or strategic document to promote the protection of human rights and fundamental freedoms by business enterprises.

31. Internet freedom also comprises positive rights and freedoms such as the right to education, which is enshrined in Article 2 of Protocol 1 to the ECHR. Indicator 1.8. addresses the issue of digital literacy as an enabler to other freedoms, and also the general promotion of access to the Internet for the purpose of education and access to culture. Digital literacy means that citizens 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.

32. 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.[9] 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.[10] Citizens should be able to freely access publicly funded research and cultural works on the Internet. [11] Access to digital heritage materials, which are in the public domain, should also be freely accessible within reasonable restrictions. Conditions on access to knowledge

---

[7] 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.
[8] 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.
[9] Committee of Ministers Declaration on human rights and the rule of law in the Information Society, CM(2005)56 final 13 May 2005.
[10] See also note 8 above, CM/Rec(2007)16 Section IV.
[11] Ibid.

are permitted in specific cases in order to remunerate right holders for their work, within the limits of permissible exceptions to intellectual property protection.

33. In addition, Recommendation *CM/Rec(2014)6* of the Committee of Ministers to member States on a guide to human rights for Internet users also provides explanations to Internet users on their human rights and fundamental freedoms online as well as their responsibilities to respect the rights of others. Verification of *Indicator 1.8.* will be the existence of State-funded digital literacy programmes, and other programmes promoting access to culture and knowledge via the Internet. Further verification will be the implementation of Council of Europe's Guide to Human Rights for Internet Users.

2. The Right to Freedom of Expression

2.1. Freedom to access the Internet

34. The EctHR has affirmed in its jurisprudence that Article 10 is fully applicable to the Internet since any restriction imposed on the latter necessarily interferes with the right to receive and impart information.[12] Hence, access to infrastructure is a prerequisite and an enabler for the realisation of the objective to guarantee freedom of expression[13]. In this context, the Council of Europe's Committee of Ministers has acknowledged that the protection of Internet infrastructure protection should be a priority.[14] To ensure that all citizens have the ability to access the Internet, the state should implement infrastructure policies to make sure that the Internet is available, accessible and affordable to all groups of the population and promote the principle of universality of the Internet.[15]

35. *Indicator 2.1.1.* is concerned with access to the Internet, and the means by which the subscriber is able to connect to it. It addresses the universal ability to access the Internet across all areas and regions of the State, irrespective of the technology used to provide that access. 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. Public service value of the Internet is understood as "people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial

[12] Yildirim v Turkey no. 3111/10, 18.03.2013;
[13] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations General Assembly 16 May 2011, S.85: "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."
[13] 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.
[13]Ibid Yildirim v Turkey, Paragaph 53.

[14] Recommendation CM/Rec (2007) 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, adopted by the Committee of Ministers on 7 November 2007 at the 1010th meeting of the Ministers' Deputies
[15] Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet

transactions) and the resulting legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing."[16]

36. Verification of this indicator would be established by positive action or measures taken by State authorities to ensure that all citizens are able to obtain an Internet connection, for example, laws or policies on universal access to the Internet, including geographic coverage of network infrastructure. Metrics could be provided by reports or studies of Internet accessibility and infrastructure coverage, or through analysis of initiatives, programmes or investments in Internet infrastructure.

37. *Indicator 2.1.2.* is based on Council of Europe Recommendation CM/Rec (2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet.[17] 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.[18] 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.

38. *Indicator 2.1.3* 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. 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. The State 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 indicator is also based on the principle of non-discrimination as enshrined in article 14 of the ECHR.

39. This indicator seeks to verify the efforts made by the State to ensure that Internet access is made available to vulnerable individuals, such as the disabled, and to minority groups. Metrics could be provided by reports on Internet accessibility, notably initiatives or programmes in support of access to the Internet for persons with disabilities and linguistic minorities.

40. *Indicator 2.1.4* is based on the jurisprudence of the ECtHR, in particular as regards the requirements on the rule of law and proportionality of measures taken by State authorities which interfere with the right to freedom of expression. When such measures are taken it is necessary that legal framework is in place which ensures both tight control over the scope of bans and effective judicial review to prevent any abuse of power. The legal framework should also include an obligation that courts assess the proportionality of measures. An effective judicial review involves also an assessment whether other less restrictive measures were possible.[19]

---

[16] CM/Rec(2007)16, section II.
[17] CM/Rec(2007)16, section II.
[18] 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.
[19] Yildirim v Turkey no. 3111/10, 18.03.2013, para 64-70.

A blanket prohibition of access to the Internet, as for instance a measure that makes networks unavailable or disrupts their functioning, is considered as incompatible with these requirements. This indicator is also concerned with the possibility that access to the infrastructure is not available on a blanket basis within a given geographic area or to a group of the population.

41. Positive verification that the requirements of this indicator are met would be provided by any law that explicitly forbids blanket prohibitions on Internet access. Transparency reports on network availability from regulators, Internet service providers or non-governmental bodies[20] would provide additional verification. Negative verification would be provided by any evidence or technical report that the Internet access is prohibited or regularly unavailable for the population of a country, or in specific regions or areas.

42. *Indicators 2.1.5 – 2.1.8.* specifically address the situation of disconnection of individuals from the Internet both in the context of implementation of a measures by the State or by an access provider. These indicators seek to verify that disconnections take place only if they are compatible with Article 10 of the ECHR. Measures which disconnect an individual from the Internet have a disproportionate impact on the right to access information and freedom of expression because they render large quantities of information inaccessible. 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[21]. Consequently, the disconnection of an Internet user could adversely affect the exercise of her/his rights and freedoms and could even amount to a violation of the right to freedom of expression, including the right to receive and impart information.[22]

43. 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. This should, nonetheless, 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. Also, the State may apply disconnection measures in penitentiary institutions ensuring compliance with Article 10 of the ECHR.

---

[20] For example, see the report 'Freedom on the Net, a global assessment of Internet and Digital Media', by Freedom House 2013.

[21] The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue has emphasized that "the Internet has become an indispensable tool for realizing 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 realization of a range of other human rights."
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

[22] The French Constitutional Court Decision of June 2009 (Conseil Constitutionel, Decision n° 2009-580 of June 10th 2009 Loi favorisant la diffusion et la protection de la création sur internet) stated that disconnection could amount to a restriction of the right to freedom of expression, including the right to receive and impart information and on that basis, that disconnection from the Internet may only be decided by a court and not be an administrative body, or any other public or private actor.

44. Every citizen, 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. If a situation arises where measures of disconnection from the Internet are not decided by a court[23], Internet users should have effective remedies against such measures, in compliance with Article 6 of the ECHR.

45. Verification of this indicator may be effected using reports by non-governmental organisations, such as those of Article 19, Center for Democracy & Technology[24], Electronic Frontier Foundation, or Freedom House.

2. 2. Freedom of opinion and the right to receive and impart information

46. *Indicators 2.2.1. and 2.2.2* addresses laws and policies of States with regard to content made available or distributed on Internet platforms and compliance with Article 10 of the ECHR. In the Internet context, the right to receive and impart information, as referred to in Article 10 of the ECHR, applies to uploading (imparting) of content, as well as to downloading or viewing or otherwise accessing content,[25] and the use of services, including anonymously.[26] 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. Internet users should be free to express their political convictions as well as their religious and non-religious views.

47. 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.[27] 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. [28]

48. Verification of this indicator would be established if laws or policies providing for restrictions on access to content, platforms and services on the Internet include specifically safeguards for the right to freedom of expression. In particular, this indicator is concerned with restrictions by means of, for example, blocking or filtering, which may be imposed via the Internet infrastructure using automated technologies (by Internet service providers or by other types of content or service providers). Verification can be assisted by reports from international human rights

[23] Examples of disconnections without a court ruling are cited in Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, United Nations General Assembly 16 May 2011, S29 – 30.
[24] For example, Centre for Democracy and Technology: "Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age," 2011.
[25] 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.
[26] Committee of Ministers Declaration on Freedom of Communication on the Internet, 28 May 2003, Principle 7.
[27] Handyside v. the United Kingdom, judgment of 7 December 1976, Series A No. 24, para.49; See also
[28] Vgt Verein gegen Tierfabriken v. Switzerland, no. 24699/94, § 45

organisations such as those of the OSCE Representative on Freedom of the Media, the UN or the EU.

49. *Indicator 2.2.3.* seeks to verify that laws or policies provide sufficient safeguards against abusive restrictive measures, notably by defining clearly and precisely the scope of such measures and providing for effective control by a court or other independent adjudicatory body[29]. It also addresses the proportionality of decisions taken by courts or independent administrative bodies regarding blocking, filtering or other restrictive measures. This indicator should be assessed in conjunction with those in section 2.4.

50. This indicator is based on the jurisprudence of the ECtHR, which has found that blocking or filtering of Internet access or content are examples of the kind of restrictions or interference which may engage freedom of expression[30]. There should be strict control of the scope of blocking and effective judicial review to prevent any abuse of power. 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. General principles with regard to blocking and filtering, based on the Court case law, have been incorporated into standards adopted by the Committee of Ministers.[31]

51. States 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[32]. 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.[33] They should be prescribed by law.

52. In this context, Internet restrictions such as blocking or filtering measures should specify clearly identifiable content, and should be based on a decision on the legality of the content by a competent national authority in accordance with the requirements of Article 6 of the ECHR. It should be possible for that decision to be reviewed by an independent and impartial tribunal or regulatory body.[34] 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[35].

53. *Indicator 2.2.3.* seeks to assess the legal basis for the technological methods by which restrictions may be imposed on Internet content. The Committee of Ministers has emphasised that "users' right to access and distribute information online and the development of new tools and services might be adversely affected by non-

---

[29]EctHR Application no. 3111/10 Yildirim v Turkey, ,Judgment, Final 18.03.2013, S.64
[30] EctHR Application no. 3111/10 Yildirim v Turkey, ,Judgment, Final 18.03.2013, Paragraph 69.
[31] 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 .
[32] Ibid CM/Rec(2008)6, see Appendix, part III, iv.
[33] Committee of Ministers Declaration on Freedom of Communication on the Internet ; Yildirim v Turkey Paragraphs 52 & 66- 68;
[34] 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 .
[35] Declaration on Freedom of Communication on the Internet, principle 3.

transparent traffic management, content and services' discrimination or impeding connectivity of devices" [36]. The Committee has emphasised its commitment to the principle of network neutrality, in order that users may have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice. Such a general principle, should apply with regard to all types of infrastructure or the network used for Internet connectivity.

54. Exceptions to this principle should be considered with great circumspection and need to be justified by overriding public interests.[37] In this context, member States paying due attention to the provisions of Article 10 of the European Convention on Human Rights and the related case law of the European Court of Human Rights, may also find it useful to refer to the guidelines of 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.

55. Verification is possible in any law, regulation or policy that addresses the conditions for blocking and filtering Internet and Internet traffic management. Also, reports by regulatory authorities in the field of telecommunications can be sources of verification.

56. *Indicator 2.2.4.* addresses the requirement for compliance with ECHR Article 6, the right to due process, in instances where restrictions are applied to Internet content. 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 non-judicial mechanisms, in addition to judicial remedies. There must be a specific legal avenue available whereby individuals can address a complaint regarding restrictions of their rights, including the length of proceedings in the determination of their rights.[38] This could be provided by a public authority, whose powers and the procedural guarantees would permit a determination whether a particular remedy is effective.[39] That authority may not necessarily be a judicial authority, but it should present guarantees of independence and impartiality.

58. States should also ensure that private actors who are mandated to implement Internet restrictions establish complaint or appeal mechanisms. Those mechanisms should be 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 of offering remedies which are in full compliance with international human rights standards directly to individuals. The United Nations Guiding Principles on Business and Human Rights provide additional guidance[40].

---

[36] Declaration of the Committee of Ministers on network neutrality (Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies)
[37] Ibid
[38] Kudla v. Poland, no. 30210/96, §157.
[39] 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.
[40] Report of the Special Representative of the Secretary- General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, 21 March 2011

59. *Indicator 2.2.5.* This indicator is concerned with the transparency of State action or measures with regard to any restrictions imposed. This is important for Internet users to be able to challenge such action or measures. States should focus on providing information to Internet users (both those who access information and those who disseminate it) and ensure that there are possibilities to challenge any restrictions imposed. Information should be given about when filtering has 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). There should be information about the manual overriding of an active filter, including contact information. [41]

60. There should be clear and transparent information regarding the means of redress available. This information could be included in terms of use and/or service or in other guidelines and policies of Internet service/online providers. It should be possible to request information and seek remediation. There should be 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. It can be verified by means of the publicly available information regarding blocking as well as by using reports authored by non-governmental organisations such as Freedom House.[42]

2.3. Freedom of the media

61. *Indicator 2.3.1.* is concerned with freedom of the media which is a corollary to freedom of expression. These freedoms are indispensable for genuine democracy and democratic processes. Editorial freedom or independence is an essential component of media freedom. [43] States have a duty to guarantee that the media can publish independently without interference. This indicator seeks to establish that this guarantee is upheld in the online context, where the notion of what constitutes 'media' has evolved. In 2011, the Committee of Ministers adopted a new notion of media[44] which encompasses all actors involved in the production and dissemination.

62. Verification of this indicator is possible if a law or policy exists that guarantees freedom of media and new media actors to produce, disseminate content and information without interference. Further sources of verification may be supplied by any report by civil society, independent organisations concerning documented cases of interference with editorial decision making, such as the OSCE reports on media freedom[45] or Reporters Without Borders "Enemies of the Internet"[46] reports or Index on Censorship media freedom reports[47] and reports from Article 19 and Freedom House.

---

[41] 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,Appendix I.i.
[42] Ibid 'Freedom on the Net, a global assessment of Internet and Digital Media', Freedom House 2013.
[43] Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media
[44] Ibid.
[45] See for example: OSCE, The Representative on Freedom of the Media, Dunja Mijatović, Regular Report to the Permanent Council for the period from 19 June through 26 November 2014, p8, p36
[46] See for example, Reporters Without Borders, 2012 Enemies of the Internet, 13 March 2012
[47] Index on Censorship: http://mediafreedom.ushahidi.com/reports

63. *Indicator 2.3.1.* seeks to verify that any licence or permission to operate as media actor on the Internet is related solely to the ability to set up in business and is not politically motivated.

64. It is based on the Recommendation of the Committee of Ministers to member States on a new notion of media, which recommends a "review of regulatory needs in respect of all actors delivering services or products in the media ecosystem so as to guarantee people's right to seek, receive and impart information in accordance with Article 10 of the European Convention on Human Rights, and to extend to those actors relevant safeguards against interference that might otherwise have an adverse effect on Article 10 rights, including as regards situations which risk leading to undue self-restraint or self-censorship." This recommendation also states that "[s]ubject to the principle that, as a form of interference, media regulation should comply with the requirements of strict necessity and minimum intervention, specific regulatory frameworks should respond to the need to protect media from interference (recognising prerogatives, rights and privileges beyond general law, or providing a framework for their exercise), to manage scarce resources (to ensure media pluralism and diversity of content – cf. Article 10, paragraph 1 *in fine*, of the European Convention on Human Rights) or to address media responsibilities (within the strict boundaries set out in Article 10, paragraph 2, of the Convention and the related case law of the European Court of Human Rights)."

65. This indicator also finds basis in Resolution 1636 (2008) "Indicators for media in a democracy" of the Parliamentary Assembly of the Council of Europe which states that "regulatory authorities for the broadcasting media must function in an unbiased and effective manner, for instance when granting licenses. Print media and Internet-based media should not be required to hold a state license which goes beyond a mere business or tax registration".

66. In addition, the Committee of Ministers declared in 2011 that privately operated media platforms should be able to operate freely[48]. Citizens rely on social networks, blogs, websites and online applications to access and exchange information, publish content, interact, communicate and associate with each other. These platforms are becoming an integral part of the new media ecosystem. Although privately operated, they are a significant part of the public sphere in that they facilitate debate on issues of public interest; in some cases, they can fulfil, similar to traditional media, the role of a social "watchdog" and have demonstrated their usefulness in bringing positive real-life change.

67. Verification may be provided by international media freedom reports, such as those from the Council of Europe's Commissioner for Human Rights, the OSCE[49], and the European Parliament report on Freedom of the Media in the Western Balkans[50] as well as reports from Article 19, Freedom House, Index on Censorship and Reporters Without Borders.

---

[48] Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, December 2011

[49] See for example: OSCE, The Representative on Freedom of the Media, Dunja Mijatović, Regular Report to the Permanent Council for the period from 19 June through 26 November 2014, p36

[50] European Parliament Directorate General for External Policies, Freedom of the Media in the Western Balkans
http://www.europarl.europa.eu/RegData/etudes/STUD/2014/534982/EXPO_STU%282014%29534982_EN.pdf

68. *Indicator 2.3.3.* seeks to verify that the State does not interfere with journalists and others who perform public watchdog functions through online media. Obstacles created by the State in order to hinder access to information of public interest may not only discourage journalists and other new media actors from fulfilling a public watchdog role[51], but may also have negative effects on their safety and security as well as on their ability to inform the public. Attacks against journalists and other new media actors constitute particularly serious violations of human rights because they target not only individuals, but deprive others of their right to receive information, thus restricting public debate, which is at the very heart of pluralist democracy.

69. The ECtHR has held that the role played by journalists in a democratic society confers upon them certain increased protections under Article 10 of the ECHR. States have a duty to create a favourable environment for participation in public debate by all persons, enabling them to express their opinions and ideas without fear.[52] To do this, States must not only refrain from interference with individuals' freedom of expression, but are also under a positive obligation to protect their right to freedom of expression against the threat of attack, including from private individuals, by putting in place an effective system of protection.

70. The Committee of Ministers has urged member States to fulfil their positive obligations to protect journalists and other media actors from any form of attack and to end impunity in compliance with the ECHR and in the light of the case law of the ECtHR. In this connection, it has also invited member States to review at least once every two years the conformity of domestic laws and practices with these obligations on the part of member States. Member States have also been encouraged to contribute to the concerted international efforts to enhance the protection of journalists and other media actors by ensuring that legal frameworks and law-enforcement practices are fully in accord with international human rights standards. The implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity is an urgent and vital necessity.[53]

71. This indicator could be verified if there are either documented cases of online threats and harassment, or documented cases of investigations and prosecutions of journalists in relation to the exercise of their activity online, such as those cited in the regular reports by the OSCE special rapporteur for Media Freedom[54] or Reporters Without Borders "Enemies of the Internet"[55] reports.

72. *Indicator 2.3.4.* seeks to verify that the confidentiality of journalists sources is protected and that they not are not subject to surveillance. Surveillance of journalists and other new media actors, and the tracking of their online activities, can endanger the legitimate exercise of freedom of expression on the Internet and can even threaten the safety of the persons concerned. It can undermine or expose their sources. In the Internet context, surveillance may entail the monitoring or storing of private communications, including the content, or gathering, storage and

---

[51] See in this regard Társaság a Szabadságjogokért v. Hungary, Application No. 37374/05, judgment of 14 April 2009, paragraph 38.

[52] Dink v. Turkey, Application Nos. 2668/07, 6102/08, 30079/08, 7072/09, 7124/09, judgment of 14 September 2010, paragraph 137

[53] Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors (*Adopted by the Committee of Ministers on 30 April 2014 at the 1198th meeting of the Ministers' Deputies*)

[54] See for example: OSCE, The Representative on Freedom of the Media, Dunja Mijatović, Regular Report to the Permanent Council for the period from 19 June through 26 November 2014, p8

[55] See for example, Reporters Without Borders, 2012 Enemies of the Internet, 13 March 2012

analysis of communications traffic data or metadata. Council of Europe's Committee of Ministers has provided guidance on these issues, notably in the Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors and Recommendation Rec(200)7 on the right of journalists not to disclose their sources of information.

73. This indicator may be verified by the existence of any law or policy that guarantees the confidentiality of journalistic sources. Further verification may be found where documented cases exist of journalists' communications and work products being monitored, such as those cited by Reporters without Borders.[56]

74. *Indicator 2.3.5.* addresses the possibility that free speech online is being challenged in new ways. For example, is based on the Committee of Ministers has expressed concern regarding distributed denial-of-service attacks against websites of independent media, human rights defenders, dissidents, whistle-blowers and other new media actors. Such attacks represent interferences with the right to impart and receive information and with the right to freedom of association. They may have a negative effect on web-hosting services that may not wish to host sensitive content. This indicator may be verified by checking any reports concerning documented cases of denial of service attacks, hacking, defacement, phishing attacks, or compromised accounts, alleged to have been committee by the State. Reporters without Borders, for example, will highlight such attacks where they exist.

75. *Indicator 2.3.6.* stems from the jurisprudence of the ECtHR and Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors. The latter states that "[e]radicating impunity is a crucial obligation upon States, as a matter of justice for the victims, as a deterrent with respect to future human rights violations and in order to uphold the rule of law and public trust in the justice system.[7] All attacks on journalists and other media actors should be vigorously investigated in a timely fashion and the perpetrators prosecuted. The effective investigation of such attacks requires that any possible link to journalistic activities be duly taken into account in a transparent manner.

76. *Indicator 2.3.7.* concerns the protection of network neutrality as an important condition for the exercise of the right to access to information or the right to freedom of expression. Internet service providers (ISPs) have the ability to manage information and data flows transiting through their networks. 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.[57] 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.[58] Verification of this indicator could be found if a positive net neutrality law or policy exists. Negative verification will be found in reports such

[56] Reporters Without Borders, 2012 Enemies of the Internet, 13 March 2012 cites several such cases
[57] See note 2 above, § 50.
[58] 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;

as those from NGOs, for example Freedom House or from Reporters without Borders, which also cover the use of traffic management to block content.

2.4. Legality, legitimacy and proportionality of restrictions

78. *Indicator 2.4.1.* asks States to verify that any restrictions are in compliance with the requirements of Article 10 paragraph 2 of the ECHR. It should be read together in sections 2.1. and 2.2. 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. [59] 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 interpretation and scope evolves with the case law of the ECtHR.

79. 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.[60] In this context, States should asses the balance of laws that restrict Internet content or access against the right to freedom of expression as enshrined in Article 10. In Neij and Sunde Kolmisoppi v. Sweden, the ECtHR has affimed that States must strike a fair balance between the competing rights concerned, as has the Court of Justice of the European Union (CJEU).[61]

80. *Indicator 2.4.2. and 2.4.3* address the specific issue of misuse of law to interfere with the right to freedom of expression and asks States to verify that their laws do not result in a violation of Article 10.

81. Laws, judicial proceedings and other measures taken by State authorities which restrict the right to freedom of expression must meet the standards of Article 10 paragraph 2 of the ECHR. They cannot be justified if their purpose is to prevent free and open public debates, legitimate criticism of public officials or the exposure of official wrongdoing and corruption. An arbitrary application of laws has a chilling effect on the exercise of the right to impart information and ideas and leads to self-censorship. [62]

82. Defamation laws, should be applied with restraint whether offline or online and should have adequate safeguards for freedom of expression. The Court has consistently applied a high threshold of tolerance for criticism where politicians, members of the government or heads of state are concerned.[63] Moreover, the Court has held that criminal sanctions applied in defamation proceedings have a disproportionate chilling effect on the exercise of journalistic freedom of expression.

---

[59] Yldirim v. Turkey, no 3111/10 § 64.
[60] Ibid. § 66-70.
[61] Ibid Neij and Sunde Kolmisoppi v. Sweden no.40397/12, Decision 19 February 2013, pp10-11; Ibid, C-70/10, Scarlet Extended S.44-49; Case C-275/06 Productores de Musica de España (Promusicae) v Telefonica de España SAU [2008]
[62] Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors, 30 April 2014, point 9.
[63] Lingens v. Austria (1986); Otegi Mondragon v. Spain (2012)

Imprisonment is recognised as a particularly severe sanction and therefore can be applied only exceptionally when the fundamental rights of other have been seriously impaired such as in cases of incitement to violence or hatred.[64] In practice, the Court has not upheld an actual sentence of imprisonment for defamation. The Parliamentary Assembly and the Commissioner for Human Rights have gone one step further by calling for decriminalisation of defamation.[65] Laws and practices providing for disproportionate awards of damages or legal costs in defamation cases may also impinge on freedom of expression.[66]

83. The Venice Commission and the Parliamentary Assembly have taken the view that pluralism, tolerance and broadmindedness in a democratic society require protection of the right to hold specific beliefs or opinions rather than protection of belief systems from criticism. The right to freedom of expression implies scrutiny, open debate and criticism, even harshly and unreasonably, of belief systems, opinions and institutions as long as this does not amount to advocating hatred against an individual or groups of people. [67]

84. Laws which criminalise the spreading, incitement, promotion or justification of hatred and intolerance (including religious intolerance) must be clear as to their application and the restrictions they impose must be proportionate to the legitimate aim pursued in line with the jurisprudence of the Court.

85. Laws on public safety and national security, including those on anti-hooliganism, anti-extremism and anti-terrorism, may restrict the right to receive and impart information both offline and online. It is therefore necessary that such laws are accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to understand what sanctions they face. These laws should also have adequate safeguards against abuse, including prompt, full and effective scrutiny of the validity of restrictions by an independent court or authority. If criminal law sanctions are imposed they must be strictly necessary and proportionate to the legitimate aim pursued as interpreted by the Court.[68]

3. The right to freedom of assembly and association

86. *Indicator 3.1.* seeks to affirm that the State guarantees the application of Article 11 of the ECHR in the context of the Internet and specifically to Internet platforms, social media and applications. The exercise of this right is not conditional upon any formal recognition of social groups and assemblies by public authorities. It includes the right to peacefully assemble and associate with others using the Internet, such as forming, joining, mobilising and participating in societal groups and assemblies, including in trade unions, using Internet-based tools. The indicator will be verified by the existence of constitutional provisions, laws, policies that are in line with international standards on freedom of assembly and association, and where it is

[64] Cumpana and Mazare v Romania (2004); Azevedo v. Portugal (2008)
[65] Resolution 1577 (2007) Towards decriminalising defamation; Human Rights in Changing Media Landscape, 2011
[66] Tolstoy Miloslavsky v UK (1995); M.G.N. Limited v UK (2004); Independent News and Media and Independent Newspapers Ireland Limited v Ireland (2005).
[67] Report on the relationship between freedom of expression and freedom of religion: the issue of regulation and prosecution of blasphemy, religious insult and incitement to religious hatred CDL-AD(2008)026 23 October 2008; PACE Recommendation 1805 (2007) Blasphemy, religious insults and hate speech against persons on grounds of their religion
[68] Ozgur Gundem v Turkey (2000); Urper and Others v Turkey (2009); Karatas v Turkey (1999); Demiral and Ates v Turkey (2008).

understood that those provisions, laws and policies guarantee that right in the context of the Internet and online communication. Negative verification may be found by consulting reports non-governmental organisations, such as the country reports published by Venice Commission or those by non-governmental organisations Article 19[69].

87. *Indicator 3.2.* seeks to affirm that associations which might be established in offline environments can use the Internet for purposes of their activities. The Joint Guidelines on Freedom of Association of the Venice Commission and OSCE/ODIHR state: "(i)n particular, new technologies have enhanced the ability of persons and groups of persons to form, join and participate in all forms of associations, including non-governmental organizations and political parties. (…) Many of the traditional activities undertaken by political parties, non-governmental organizations and other associations can be exercised online. These activities can include registering, gathering signatures, fundraising and making donations."[70]

88. Also, individuals should be able to participate in local, national and global public policy debates online, including the free discussion of legislative initiatives and public scrutiny of State decision-making. The indicator is based on Committee of Ministers' recommendations on the public service value of the Internet, which encourage the use of online forums, weblogs, political chats, instant messaging and other forms of citizen-to-citizen communication online, 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.[71] An example of the online application of Article 11 in this context, would be the signing of a petition or the participation in a campaign of civic action**.**

89. A form of verification of this indicator would be to assess the development and implementation of strategies for e-democracy, e-participation and e-government using the Internet and internet-based platforms such as social media or other online services, in democratic processes and debates, as recommended by the Committee of Ministers.[72] Such e-democracy strategies could be applied both in relationships between public authorities and civil society, as well as in the provision of public services.

90. *Indicators 3.3. and 3.4.* seek to verify that any restriction on Internet platforms, social media or other online services that facilitate assembly and association complies with Article 11 of the ECHR. In this context, States should take note that the principles established by the ECtHR regarding the protection of political speech under Article 10, also apply to Article 11. In Wingrove v. the United Kingdom, the ECtHR asserted that there is little scope under for State restrictions on either political speech or debates of questions of public interest.[73] Verification would be established if there are no laws or policies, nor any other measures, imposing restrictions on access to or use of Internet platforms, social media or other online services for the

[69] http://www.article19.org/resources.php
[70] Joint Guidelines on Freedom of Association of the European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), 2014, § 260.
[71] Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, p4.
[72] Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, Appendix, part I.
[73] Wingrove v. the United Kingdom, 25 November 1996, § 58, Reports 1996-V.

purpose of associating with others or creating communities of interest. Verification could be that a restriction has been prescribed by law, with provision for judicial or administrative oversight, including the right to be heard.

4. The right to a private life

4.1. Personal data protection

91. *Indicator 4.1.1* asserts the right to a private and family life, home, and correspondence. This right must be guaranteed by States in compliance with Article 8 of the ECHR. It is interpreted by the case-law of the ECtHR and complemented and reinforced by the Council of Europe Convention 108. The right to private correspondence includes mail and telephone communications, as established in the case of Klass v Germany.[74] In Copland v United Kingdom, the ECtHR has interpreted Article 8 to encompass email correspondence, including in the workplace, as well as information derived from personal internet usage[75]. It has further stated that private life relates to a person's right to their image[76], 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. [77]

92. *Indicator 4.1.2.* addresses the protection of personal data, as defined in Convention 108 for the Protection of Individuals with Regard to the Processing of Personal Data[78]. The indicator seeks to verify that States have assured the protection of personal data within the wider scope of their obligation to safeguard the right to private and family life. The protection of personal data therefore plays a fundamental role in the exercise of the right to respect for private and family life enshrined in Article 8, whereby national legislation must provide appropriate safeguards to prevent any use of personal data which does not comply with the guarantees provided for in this article and to ensure the effective protection of recorded personal data against misuse and abuse.

93. *Indicator 4.1.3.* seeks to verify that the principles and rules of Convention 108 are respected by public authorities and private companies. Personal data must be obtained and processed fairly and lawfully, and stored for specified and legitimate purposes. Data should 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.[79]

94. Emphasis is placed on two specific principles of the processing of personal data: the lawfulness of the processing, and the user's consent. Convention 108 establishes

---

[74] Klass and Others v. Germany, no 5029/71, §41.
[75] Copland v United Kingdom, Application no. 62617/00. 3 April 2007, paragraph 41-42
[76] Von Hannover v. Germany (no. 2), nos. 40660/08 and 60641/08 §§ 108-113.Sciacca v. Italy, no. 50774/99, § 29.
[77] 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).
[78] Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (ETS No.108) Article2. Note that the Propositions of Modernisation adopted 18.12. 2012 have updated the Convention *inter alia* for the Internet context.
[79] See Convention 108, Article 5.

that users should be able to exercise control over their personal data, notably that they have 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, rectification or erasure is not complied with.[80]

95. Convention 108 encompasses all forms of data processing that may take place in the context of the Internet - both network and content - such as collection, storage, alteration, erasure and retrieval or dissemination or personal data.[81] In practice, this could include the automatic processing of personal data regarding the use of browsers, e-mail, instant messages, voice-over Internet protocols, social networks and search engines as well as cloud data storage services.

96. Informed consent is underlined 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, or used in ways other than those necessary for the specified purposes for which they were originally collected. Social network users should be able to "opt in" to permit 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. This indicator may be verified by the existence of any law that addresses the processing of personal data and incorporates the principles and safeguards enshrined in Convention 108. The free, specific, informed and explicit (unambiguous) consent to the processing of personal data on the Internet is asserted in the Propositions of Modernisation to Convention 108 adopted 18.12. 2012.[82]

97. *Indicators 4.1.4. - 4.1.7.* seek to verify that individuals are capable of exercising their rights in the context of personal data processing. 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.[83] In the context of profiling[84], 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

[80] See Convention 108, Articles 8 & 10.
[81] See Convention 108, Article 2.
[82] The 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."
[83] See Convention 108, Article 8
[84] 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 Profiling is understood as automatic data processing techniques that consist of analysing an Internet user's personal preferences, behaviours and attitudes in order to take decisions concerning him or her, for example to predict future behaviour or supply targeted advertisements.

safeguarding the legitimate interests of the Internet user are in place. [85]Verification may be carried out by for example examining the compatibility of the terms and conditions of service and platform providers with the law and with the requirements of Article 8.

98. *Indicator 4.1.6.* in particular concerns the issue of anonymity. This is based on the case law of the ECtHR, the Budapest Convention and other instruments of the Committee of Ministers. The ECtHR 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 ECtHR 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.[86]

99. 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."[87]

100. The Council of Europe's Committee of Ministers affirmed the principle of anonymity in its Declaration on Freedom of Communication on the Internet. [88]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.

101. This indicator may be negatively verified by the existence of any law or policy prohibiting Internet users to use encryption software to protect their communications, or by any law or policy restricting the use of encryption or other security software or enabling the government agencies to have access to encryption keys and algorithms. Positive verification entails the absence of such laws or policies.

4.2. Freedom from surveillance

[85] 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
[86] K.U. v. Finland, no. 2872/02 § 49.
[87] Budapest Convention on Cybercrime, Article 2, explanatory report, §. 62.
[88] See Declaration on Freedom of Communication on the Internet, Principle 7.

102. *Indicator 4.2.1.* draws on the jurisprudence of the ECtHR. It seeks to verify that all surveillance measures comply with Article 8 of the ECHR and are subject to independent and impartial oversight. Surveillance measures can be both general (mass surveillance) or targeted. The ECtHR has interpreted Article 8 such that the concept of correspondence covers mail and telecommunications[89] as well as e-mails[90]. The interpretation of this concept of correspondence is evolving to keep pace with technology development. Guaranteeing the confidentiality of communications entails protecting them from all forms of surveillance, including interception. In the context of the Internet, surveillance relates to the listening to, recording, monitoring or storing of private communications. It may involve securing the content of data – this could be done by obtaining covert access to systems, or by means of electronic eavesdropping or tapping devices. Surveillance in the Internet context may additionally entail the gathering, storage and analysis of communications traffic data or metadata. This is data which does not reveal the content of the communication, but does reveal the sender, transmission details, and subject of it.

103. The ECtHR interpreted Article 8 of the ECHR in the context of surveillance cases has pronounced itself on the importance of supervision of surveillance measures by authorities other than those who carry out such measures. Although the cases reviewed by the ECtHR do not concern Internet technologies the principles established therein are valid in the context of the Internet. This is based on the general principle established by the ECtRH that "[it] must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse".[91] The review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated.[92] The ECtHR has derived from the general principle of the rule of law that, in the context of surveillance, an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.[93]

104. *Indicator 4.2.2.* seeks to verify that any form of State interception or surveillance of private correspondence or activities on the Internet must have a basis in law. However, 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. Hence, the very existence of legislation permitting surveillance of telecommunications may be considered as an interference with the right to private life. The EctHR has 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.[94]

---

[89] 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.
[90] See Copland v. UK, no 62617/00, paragraph 41.
[91] Klass others v. Germany, no 5029/71, paragraph 50.
[92] Klass others v. Germany, no 5029/71, paragraph 55
[93] Klass others v. Germany, no 5029/71, paragraph 55
[94] 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.

105. These principles established by the ECtHR make particular reference to the requirements that should be met by any law that provides for covert measures of surveillance of correspondence and communications by public authorities. The law should have detailed rules on minimum safeguards for the exercise of discretion by public authorities. These minimum safeguards include 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; (vi) the circumstances in which data obtained may or must be erased or the records destroyed.[95]

106. Verification of this indicator is therefore done on the basis not only of the existence of a law, but also of the quality of the law, which must incorporate safeguards against abuse[96]. It should enshrine the principle of foreseeability, namely that 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 covert and potentially harmful interference with the right to respect for private life and correspondence.[97] Verification may be obtained from reports of international organisations, bodies such as the Council of Europe Commissioner for Human Rights, the Venice Commission, the United Nations special rapporteur on freedom of expression as well as NGOs such as Reporters without Borders, Freedom House, Article 19, and Index on Censorship.

107. *Indicator 4.2.2.* seeks to establish that any law or policy implementing surveillance measures will pursue a legitimate public policy aim in line with those Article 8 paragraph 2. This aim should be precisely defined and narrow in scope. This indicator also refers to paragraph 2 of Article 8 which requires that any surveillance law or policy, or order, is necessary in a democratic society[98]. This means that it should be proven that there is a pressing social need for it, and that it is the least restrictive means for achieving that aim. The necessity of such a law requires that the aim is balanced against competing rights and freedoms. The indicator seeks to establish that such a balancing process has been conducted.

108. This indicator draws from the ECtHR jurisprudence, which has underlined that such measures can only be considered "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse'.[99] The ECtHR held that although measures which interfere with privacy may be designed to protect democracy, they carry with them an inherent possibility for abuse of power that could have harmful consequences for democracy as a whole. Negative verification may be obtained from reports covering State surveillance that appears not to pursue a legitimate aim. These reports may come

---

[95] 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.
[96] Ibid Kopp v Switzerland, paragraphs 62-66
[97] 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.
[98] See Malone v United Kingdom paragraph 81-82
[99] Judgment of 2 August 1984, Malone v. the United Kingdom, European Court of Human Rights (Plenary), No. 8691/79 Series A, paragraph 81

from international organisations as well as NGOs, for instance Article 19, Freedom House, Index on Censorship and Reporters Without Borders.

109. *Indicator 4.2.3.* is based on the jurisprudence of the ECtHR which requires that whenever a State puts in place a system of surveillance there are effective guarantees against abuse. The ECtHR has acknowledged that the States enjoy a certain margin of appreciation in assessing the existence and extent of such necessity, but this margin is subject to European supervision. The ECtHR has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the interference to what is necessary in a democratic society.[100]

110. This indicator focuses on the prior authorisation of surveillance measures. The ECtHR has expressed a preference for judicial authorisation of surveillance measures.[101] Despite the fact that the ECtHR has not made prior judicial authorisation a requirement applicable to all cases, its jurisprudence clearly requires that the body authorising surveillance measures should be independent of the service carrying out surveillance measures and the executive.[102]

111. Verification of this indicator may be found in the existence of mechanisms for supervision and review by competent authorities, such as Parliamentary committees or other public bodies responsible for such oversight. These public bodies should be independent of the executive and of any authorities charged with conducting surveillance.

112. *Indicators 4.2.5. to 4.2.7.* seek to verify that there is adequate oversight of surveillance measures during or after the phase of their implementation. These are derived from the criteria that the ECtHR has used to asses whether or not oversight arrangements provide sufficient safeguards to prevent abuse. The ECtHR has consistently held that the review of surveillance measures should be done by an independent body.[103] There must be a legal basis which explains how such supervision is carried out.[104] The ECtHR had identified competences of oversight bodies that would be relevant to an assessment of effective safeguards against abuse. Among the criteria that the ECtHR has examined is whether oversight bodies have access to all relevant information, including classified information and whether they have the power to quash surveillance orders and require that the material obtained through surveillance measures is destroyed.[105]

113. *Indicators 4.2.8 to 4.2.10.* are drawn from the recommendations of the Council of Europe Human Rights Commissioner regarding the democratic oversight of national security services. The Commissioner stresses that the mandate of such bodies should include scrutiny of human rights compliance of security services co-operation with foreign bodies, including co-operation through the exchange of information, joint operations and the provision of equipment and training. External oversight of such co-operation with foreign bodies should include, "a. ministerial

[100] Klass and others v. Germany, paragraph 54-56; Kennedy v. the United Kingdom, paragraph 154.
[101] Klass and others v. Germany, para 56 "[t]he Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."
[102] Dumitru Popescu v Romania, para. 70-73, Klass and others v. Germany para 56; Kennedy v. the United Kingdom, para. 167.
[103] CASE OF ASSOCIATION FOR EUROPEAN INTEGRATION AND HUMAN RIGHTS AND EKIMDZHIEV v. BULGARIA para. 85-87.
[104] Iordachi and others v. Moldova,para. 49.
[105] Kennedy v. the United Kingdom, para.166; 167.

directives and internal regulations relating to international intelligence co-operation; b. human rights risk assessment and risk-management processes relating to relationships with specific foreign security services and to specific instances of operational co-operation; c. outgoing personal data and any caveats (conditions) attached thereto; d. security service requests made to foreign partners: (i) for information on specific persons; and (ii) to place specific persons under surveillance; e. intelligence co-operation agreements; f. joint surveillance operations and programmes undertaken with foreign partners."[106]

114. Verification may be found in the existence of mechanisms for supervision and review by competent authorities, such as Parliamentary committees or other public bodies responsible for such oversight.

5. Remedies

115. *Indicator 5.1.* seeks to verify that Internet users are able to exercise their 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 ECtHR, 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. The ECtHR, 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).

116. There should be a national authority tasked with arbitrating on allegations of such violations of the rights guaranteed.[107] 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.[108] 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, to sanction any violation and to guarantee the victim that the decision taken will be executed. The legal procedure should be complemented by a specific legal avenue available whereby an individual can complain about the unreasonable length of proceedings in the determination of his/her rights.[109]

117. *Indicators 5.2. and 5.3.* seek to verify that the right to an effective remedy as enshrined in Article 13 of the ECHR is respected. Everyone whose rights and freedoms are restricted or violated on the Internet has the right to an effective remedy. These indicators are based on the jurisprudence of the ECtHR. States, as

---

[106] CommDH/IssuePaper(2015)2 05 June 2015 Democratic and effective oversight of national security services.
[107] 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.
[108] 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.
[109] Kudla v. Poland, no. 30210/96, §157.

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. This indicator concerns ECHR Article 13, which 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. Article 13 requires the provision of a domestic remedy to deal with the substance of a complaint under the ECHR and to grant appropriate relief.[110] 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.[111]

118. The remedy must be effective in practice and in law and not conditional upon the certainty of a favourable outcome for the complainant.[112] Although no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided in law may do so. [113] Effective remedies should be available, known, accessible, affordable and capable of providing appropriate redress. Public authorities and/or other national human rights institutions may be in a position to apply an effective remedy. In the context of the Internet, broadband service providers may also be in a such a position, but they do not enjoy sufficient independence to be compatible with Article 13 ECHR.

119. *Indicator 5.4.* seeks to verify the implementation of the United Nations Guiding Principles on Business and Human Right, which 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. [114]

120. Verification may be sought in the terms of use and services of Internet platforms with a view to establishing whether Internet users are offered clear and transparent information regarding the means of redress available to them. 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

---

[110] Kaya v. Turkey, no. 22729/93, §106.
[111] Smith and Grady v. UK, no 33985/96 33986/96.
[112] Kudla v. Poland, no. 30210/96, §158.
[113] 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.
[114] 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.

communications, citizens' advice offices, human rights or digital rights associations or consumer organisations.

121. Other sources of verification include transparency reports issued by the Internet Service Providers or by the Internet platforms. Google provides Transparency reports[115] detailing removal requests from its search engine, blogging platform and YouTube. The removal requests come from State authorities and law enforcement, and from copyright holders. With regard to copyright, Google provides names of those making the request and the requested URL. With regard to government removal requests, Google provides generic information, without disclosing any names. Twitter publishes transparency reports regarding law enforcement and government requests for removal of content, and also reports on requests for removal of content under US copyright law. Twitter provides aggregated figures only, with no details of the individual requests.[116] Vodafone provides a country-by-country-disclosure report on the assistance that it provides to law enforcement, with additional details on certain countries in an Annexe[117]. It provides information on how it handles requests for content removal, following the UN guidelines for business and human rights,[118] but it does not disclose the actual requests. Other sources of verification may be reports from international human rights organisations that have analysed Internet blocking orders.

122. Transparency reports provided by intermediaries provide some means of verification, although the actual data published may be limited to total numbers of requests made and the number of requests complied with. Google provides Transparency reports[119] detailing the number of government requests for information about its users.[120] Twitter publishes transparency reports on law enforcement and government requests for data related to its users[121]. Facebook discloses transparency reports on law enforcement requests[122] for personal data of its users. Vodafone provides a transparency report on which governments require it to disclose communications traffic data[123] and the legal basis for doing so.

[115] http://www.google.com/transparencyreport/
[116] https://transparency.twitter.com/
[117] Vodafone.com Country-by-country disclosure of law enforcement assistance demands http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html
[118] See: Human Rights Council Resolution on Human rights and transnational corporations and other business enterprises A/HRC/RES/17/4,
[119] http://www.google.com/transparencyreport/
[120] http://www.google.com/transparencyreport/userdatarequests/?hl=en
[121] https://transparency.twitter.com/
[122] https://www.facebook.com/about/government_requests
[123] http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf