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)07
30 September 2015

Report of the 4th MSI-INT meeting
7-8 September 2015
Strasbourg, Agora Building, Room G04

Opening of the meeting and information by the Secretariat

1. The Chair of the MSI-INT opened the meeting. Mr Patrick Penninckx, Head of Information Society Department, addressed the meeting and informed the participants about the state of play with regard to the draft recommendation on the free, transboundary flow of information on the Internet which was adopted by the Committee of Ministers on 1 April 2015. The draft recommendation on network neutrality was finalised by the Steering Committee on Media and Information Society (CDMSI) at its last meeting (16-19 June 2015) and was transmitted to the Committee of Ministers for possible adoption.

3. Mr Penninckx also informed the MSI-INT about the Secretary General's Report "The State of Democracy, Human Rights and the Rule of Law in Europe 2015", which had a chapter on freedom of expression. A comparative study on blocking, filtering, removal of Internet content in the 47 member States was being prepared together with the Swiss Institute of Comparative Law. In addition, the MSI-INT was informed about the Conference 'Freedom of expression – still a precondition for democracy?' which will take place in Strasbourg on 13 - 14 October.

4. In respect of the draft recommendation on Internet freedom, Mr Penninckx informed the MSI-INT that the CDMSI, at its last meeting (16-19 June 2015) had expressed support to the approach taken by the expert committee in its draft. CDMSI members had also provided comments during and after its meeting.

5. The agenda was adopted without any changes as it appears in Appendix 1. The list of participants appears in Appendix 2. The gender distribution of the 24 participants was 14 men (59%) and 10 women (41%).

Draft recommendation on Internet freedom

6. The Secretariat informed the MSI-INT about the results of the multi-stakeholder consultations held between 8 April 2015 and 11 May 2015 and about the comments provided by the CDMSI between 19 June 2015 and 31 July 2015. The MSI-INT took note of these comments as they appear in documents *CDMSI(2015)Misc04* and *MSI-INT(2015)Misc.*

The MSI-INT expressed general satisfaction with how these comments were reflected in the revised draft recommendation and continued to work on this basis.

7. The Russian Federation proposed to introduce the following text in the 1st indent, paragraph 7 of the operative part of the draft recommendation:

" – Coordinate measures aimed at finding a solution to the following issues within the framework of the UN/ITU:

1) **Internet internationalization**:
2) Enhancement of the governments' role in participation in the process of Internet governance;
3) Ensuring equal rights of States in Internet governance;
4) Ensuring the sovereign right of States to regulate their national Internet segments;
5) Development of global policy in the field of Internet governance at intergovernmental level."

8. The MSI-INT took note of this proposal and agreed that, for the purpose of this draft recommendation, the aspects of Internet governance are sufficiently addressed in paragraph 4 of its preamble. The MSI-INT decided that the proposal should be recorded in the report of the meeting, while underlining that discussion of these issues would be more appropriate to take place in the CDMSI, which is in the process of developing a draft Internet governance strategy 2016-2019.

9. The MSI-INT discussed extensively the wording of the Internet freedom indicators and agreed on a number of changes. The Secretariat was instructed to reflect in the explanatory memorandum to the draft recommendation the elements which were agreed not to be included in the draft recommendation. In respect of the issues related to Internet intermediaries, the MSI-INT discussed the desirability of addressing them in the present draft recommendation. In light of the judgement of the European Court of Human Rights in the case of Delfi v. Estonia and taking into account possible future work in the Council of Europe, the MSI-INT agreed to recommend that issues related to the roles and responsibilities of Internet intermediaries should be part of a fully-fledged and dedicated reflection and analysis. The MSI-INT decided to submit the revised draft recommendation, as it appears in Appendix 3, to the CDMSI for approval and possible transmission to the Committee of Ministers for adoption. The MSI-INT also agreed that the draft explanatory memorandum should be updated by the Secretariat on the basis of discussions during the meeting.

Draft report on freedom of assembly and association on the Internet

15. The Secretariat informed the MSI-INT about the comments received from CDMSI members and how these were reflected in an updated version of the draft report. The MSI-INT took note of the comments as they appear in document *MSI-INT(2015)Misc2.* The delegation of the Russian Federation proposed to include in the draft report the wording contained in paragraph 7 above. The MSI-INT took note of this proposal and decided that, based on the same reasons explained in paragraph 8 above, the proposal would be integrated in the report of the 4th meeting of the MSI-INT. Furthermore, it was agreed that whenever Council of Europe member States are mentioned in the report there should be specific references to Council of Europe sources rather than other organisations' sources. The MSI-INT agreed on the draft report as it appears in Appendix 4 and decided that it should be updated by the Secretariat on the basis of the discussions at the meeting. Thereafter, it should be transmitted to the CDMSI to be taken note of.

16. No other business was discussed.

Appendix 1

Annotated Agenda[1]

1. Opening of the meeting

The Chair will open the meeting.

2. Adoption of the agenda

3. Information by the Secretariat

The Secretariat will provide information of relevance to the work of the MSI-INT, in particular on the last meeting of the Steering Committee on Media and Information Society (CDMSI).

4. Draft recommendation on Internet freedom

The MSI-INT is expected to finalise and decide to transmit the draft recommendation to the CDMSI for approval. The MSI-INT is also expected to take note of the draft explanatory memorandum to the draft recommendation.

- Draft recommendation CM/Rec__ of the Committee of Ministers to member states on Internet freedom (*MSI-INT(2014)13 rev3*);
- Draft explanatory memorandum to the draft recommendation CM/Rec__ of the Committee of Ministers to member States on Internet freedom (*MSI-INT(2015)06*);
- Compilation of comments on the draft recommendation on Internet freedom, 18 May 2015 (CDMSI(2015)Misc04);
- Compilation of comments by CDMSI and MSI-INT members on the draft recommendation, 28 August 2015 (*MSI-INT(2015)Misc*).

5. Draft report on freedom of assembly and association on the Internet

The MSI-INT is expected to finalise and decide to transmit the draft report to the CDMSI to be taken note of.

- Draft report on freedom of assembly and association on the Internet(*MSI-INT(2014)08 rev3*);
- Compilation of comments by CDMSI and MSI-INT members on the draft report, 28 August 2015 (*MSI-INT(2015)Misc2*).

6. Any other business

[1] Document as contained in document MSI-INT(2015)05, dated 28 August 2015

Appendix 2
List of participants

MSI-INT MEMBERS

Mr Garegin CHUGASZYAN, Executive Director, Information Technologies Foundation (ITF), Yerevan (Armenia) (*apologised*)

Mr Vlasios DOUMPIOTIS (Dr), Head of the Department "Information Data Entry", Directorate of Information Technology Systems, Secretariat General of Information and Communication - Secretariat General of Mass Media, Athens (Greece)

Dr Michael KOGLER, Deputy Head of Department for Media Law, Constitutional Service of the Federal Chancellery (Austria) (*apologised*)

Ms Zlatina NIKOLOVA, Chief Expert, European Programmes and Projects Department, Ministry of Transport, Information and Communications Technology (Bulgaria)

Mr Oliver SCHENK, Legal Adviser, International Media Cooperation Division, Office of the Federal Government Commissioner for Culture and the Media (BKM) (Germany) (Chair)

Ms Margrét MAGNÚSDÓTTIR, Legal Advisor in the field of Media, Ministry of Education, Science and Culture (Iceland) (Vice-Chair)

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

Mr Yaman AKDENIZ, Professor of Law (Faculty of law), Pro-Rector for the Istanbul Bilgi University (*apologised*)

Mr Alexander BORISOV, Professor, Moscow State Institute of International Relations

Ms Maeve DION, Swedish Law and Informatics Research Institute, Faculty of Law, Stockholm University (*apologised*)

Ms Gabrielle GUILLEMIN, Legal officer - Freedom of Expression, Media Regulation, Freedom of Information - Article 19, London

Dr Monica HORTEN, Visiting Fellow, London School of Economics and Political Science

Ms Karmen TURK, Advocate, Triniti Tallinn

PARTICIPANTS

Council of Europe Member States

Ms Susanna ADAMYAN, Permanent Representation of Armenia to the Council of Europe

Mr Bakhtiyar MAMMADOV, Head of Legal and Human Resources Department, Ministry of Communications and High Technologies (Republic of Azerbaijan)

Mr Mikhail MEDRISH, Chairman of the Council (Board) of the Coordination Center for the Russian ccTLD (Russian Federation)

Mr Nicolai MURASHOV, Expert, Federal Security Service, Moscow (Russian Federation) (*apologised*)

Mr Arseny Nedyak, Deputy Director – Department of State Policy in the field of Mass Media, Ministry of Communications and Mass Media, Moscow, Russian Federation

Ms Svetlana VOLKOVA, Expert, Federal Security Service, Moscow (Russian Federation) (*apologised*)

Mr Veniamin YARKIN, Aide to the Special Representative of the President of the Russian Federation on International Cooperation on Information Security, Attaché, Department of new challenges and threats, Ministry of Foreign Affairs, Moscow (Russian Federation)

Dr Simona KRALJ-ZATLER, Under-Secretary, Information Society Directorate, Ministry of Education, Science and Sport (Slovenia) (*apologised*)

Mr Nicolas ROLLIER, International Relations Service Federation Office of Communication, Federal Department for the environment, transport, energy and communication (Switzerland / Suisse)

Mr Özgür Fatih Akpinar, Turkish Information Communication Authority, Ankara (Turkey)

Mr Hidayet Yıldız, NRA Board Member, Turkish Information Communication Authority, Ankara, (Turkey)

International Organisations

Mr Mario OETHEIMER, European Union Agency for Fundamental Rights, Vienna (*apologised*)

Ms Xianhong HU, Programme Specialist, Section for Freedom of Expression, Division for Freedom of Expression, Democracy and Peace - Communication and Information Sector, UNESCO

Mr Maciej TOMASZEWSKI, European Commission, DG-CONNECT (Unit G1 on Converging Media) (*apologised*)

Mr Michael UNLAND, Organisation for Security and Cooperation in Europe (*apologised*)

Civil society, private sector and other communities

Mr Bertrand de la CHAPELLE, Director, Internet & Jurisdiction Project (*apologised*)

Mr Paul FEHLINGER, Manager, Internet & Jurisdiction Project (*apologised*)

Mr Marc VAN DER HAM, Google Public Policy (*apologised*)

Mr Marco PANCINI, Google Public Policy (*apologised*)

Ms Siobhan CUMMISKEY, Policy Manager EMEA, Facebook (*apologised*)

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

Mr Michael ROTERT, Honorary Spokesman, EuroISPA (European Internet Service Provider Association)

Council of Europe Secretariat

Mr Patrick PENNINCKX, Head of Information Society Department

Ms Elvana THAÇI, Secretary to the MSI-INT Committee, Administrator, Media Division, Information Society Department

Ms Ana GASCON-MARCEN, Administrator, Media Division, Information Society Department

Ms Elisabeth MAETZ, Assistant, Media Division, Information Society Department

Appendix 3

Draft Recommendation CM/Rec(2015)__ of the Committee of Ministers to member states on Internet freedom

(*adopted by the Committee of Ministers on _____ 2015 at the __th meeting of the Ministers' Deputies*)[2]

1. The European Convention on Human Rights (hereinafter the ECHR) applies both offline and online. The Council of Europe member States have negative and positive obligations to respect, protect and promote human rights and fundamental freedoms on the Internet.

2. Internet freedom should be considered as part of a proactive approach to implement the ECHR and other Council of Europe standards with regard to the Internet by Council of Europe member States. Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection in compliance with the ECHR. The Council of Europe's member States' understanding of Internet freedom should be a comprehensive one and firmly grounded on the ECHR.

3. Internet governance arrangements, whether national, regional or global, must build on this understanding of Internet freedom. States have rights and responsibilities with regard to international Internet-related policy. In the exercise of their sovereignty rights, States must, subject to international law, refrain from any action that would directly or indirectly harm persons or entities inside and outside of their territorial jurisdiction. Any national decision or action restricting human rights and fundamental rights on the Internet must comply with international obligations and in particular be based on law, be necessary in a democratic society, fully respect the principles of proportionality and guarantee access to remedies and the right to be heard and appeal with due process safeguards.

4. As part of their obligation to secure to everyone within their jurisdiction the rights and freedoms enshrined in the ECHR, States should create an enabling environment for Internet freedom. To this end it is recommended that States carry out regular evaluations of the Internet freedom landscape at the national level with a view to ensuring that the necessary legal, economic and political conditions are in place for Internet freedom to exist and develop. Such evaluations contribute to a better understanding of the application of the ECHR to the Internet in member States and to its better implementation by national authorities.

5. The ECHR and Council of Europe standards provide benchmarks and references for national evaluations of Internet freedom. They can be conceptualised as indicators which guide and enable member States to identify existing or potential challenges to Internet freedom, as an analytical framework to evaluate the implementation of human rights standards on the Internet and as a reference for developing international policy and approaches relating to the Internet.

6. The Council of Europe has a key role to play in promoting Internet freedom in Europe and globally. Building on member States' national evaluations, the Council of Europe can observe the evolution of regulatory frameworks and other developments in its member States and provide regular overviews on the challenges to Internet freedom in Europe. This

[2] As contained in document MSI-INT(2014)13rev5, dated 8 September 2015

would be a good basis for further development of Council of Europe Internet-related policies.

7. The Committee of Ministers recommends that member States:

- periodically evaluate the respect and implementation of human rights and fundamental freedom standards with regard to the Internet using the indicators included in this recommendation, with a view to elaborating national reports, wherever appropriate;

- ensure the participation of all stakeholders from private sector, civil society, academia and the technical community in their respective roles in the evaluation of the state of Internet freedom and development of national reports;

- consider sharing on a voluntary basis information or national reports on Internet freedom with the Council of Europe;

- be guided by and promote these indicators when participating in international dialogue and international policy-making on Internet freedom;

- take appropriate measures to promote the United Nations "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework.

8. The Committee of Ministers also invites the Secretary General of the Council of Europe to reflect on issues related to Internet freedom in his annual report on the state of democracy, human rights and the rule of law in Europe, with a special emphasis on the sharing of best practices. Such reflection should build also on national evaluations of member States.

INTERNET FREEDOM INDICATORS

Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection in compliance with the ECHR. These indicators focus on the right to freedom of expression, the right to freedom of assembly and association, the right to private life and the right to an effective remedy. They build on the existing and established human rights standards and enforcement mechanisms. A comprehensive approach to Internet freedom considers all indicators. They are intended to provide guidance in conducting a qualitative and objective evaluation of and reporting on Internet freedom in Council of Europe member States. They are not designed to rate the levels of Internet freedom or as a means of comparing countries.

1. An enabling environment for Internet freedom

1.1. The protection of human rights and fundamental freedoms on the Internet is guaranteed in law in full compliance with the ECHR.

1.2. State interference with the exercise of human rights and fundamental freedoms on the Internet complies with the ECHR.

1.3. Laws and policies relating to the Internet are assessed at the stage of their development with regard to impact that their implementation may have on the exercise of human rights and fundamental freedoms.

1.4. Laws and policies relating to the Internet are developed by State authorities in an inclusive and transparent process which enables the participation of all stakeholders, including the private sector, civil society, academia and the technical community.

1.5. Any state body which has regulatory or other competence over Internet matters carries its activities free from political or commercial interference, in a transparent manner and protects and promotes Internet freedom.

1.6. The State protects individuals from cybercrime through effective criminal justice or other measures. Where such measures risk interference with the right to private life, the right to freedom of expression or the right to freedom of peaceful assembly and association they are subject to conditions and safeguards against abuse. These measures comply with Articles 8, 10 and 11 of the ECHR, notably they are prescribed by law, which is precise, clear, accessible and foreseeable, pursue a legitimate aim, are necessary and proportionate in a democratic society and allow for effective remedies.

1.7. The State develops policies and takes measures to implement the United Nations "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework".

1.8. The State provides digital literacy programmes for users to foster their ability to make informed decisions and to respect the rights and freedoms of others. The state promotes access to and use of educational, cultural, scientific, scholarly and other content.

2. The right to freedom of expression

2.1. Freedom to access the Internet

2.1.1. The Internet is available, accessible and affordable to all groups of population without any discrimination.

2.1.2. The public has access to the Internet in facilities supported by public administration (Internet access points), educational institutions or private owners (universal community service).

2.1.3. The State takes reasonable measures to ensure access to the Internet to those with low income, in rural or geographically remote areas and those with special needs such as persons with disabilities.

2.1.4. There are no general nation-wide restrictions on access to the Internet except when this is in compliance with Article 10 of the ECHR.

2.1.5. The State recognises in law and in practice that disconnection of individuals from Internet, as a general rule represents a disproportionate restriction of the right to freedom of expression.

2.1.6. Any restriction of Internet access, including in penitentiary institutions, complies with the conditions of Article 10 of the ECHR regarding the legality, legitimacy and proportionality of

restrictions with freedom of expression and the positive obligation of the State to protect the right to freedom of expression.

2.1.7. Before Internet access restrictive measures are applied, a court or independent administrative authority determines that disconnection from Internet is the least restrictive measure for achieving the legitimate aim. The continuing necessity of the restrictive measure is evaluated by these authorities on a continuing basis. These conditions do not apply to cases of non-payment by users for their Internet services.

2.1.8. When restrictive measures are applied, the person concerned has the right to due process before a court or an independent administrative authority whose decisions are subject to judicial review, including the right to be heard and the right of appeal in compliance with Article 6 of the ECHR.

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

2.2.1. Any measure taken by State authorities or private sector actors to block or otherwise restrict access to an entire Internet platform (social media, social networks, blogging or any other website) or ICTs tools (instant messaging or other applications) or request by State authorities to carry out such actions, complies with the conditions of Article 10 of the ECHR regarding the legality, legitimacy and proportionality of restrictions.

2.2.2. Any measure taken by State authorities or private sector actors to block, filter or remove Internet content, or any request by State authorities to carry out such actions complies with the conditions of Article 10 of the ECHR regarding the legality, legitimacy and proportionality of restrictions.

2.2.3. Internet service providers treat Internet traffic equally and without discrimination on the basis of sender, receiver, content, application, service or device. Internet traffic management measures are transparent, necessary and proportionate to achieve overriding public interests in compliance with Article 10 of the ECHR.

2.2.4. Internet users or other interested parties have access to an appeal procedure compliant with Article 6 of the ECHR with regard to any action taken to restrict their access to the Internet or their ability to receive and impart content or information.

2.2.5. The State provides information in a timely and appropriate manner to the public about restrictions it applies to the freedom to receive and impart information, such as explanation at the website which was blocked or from which information was removed, including details of the legal basis, necessity and justification for such restrictions, the court order authorising them and the right to appeal.

2.3. Freedom of the media

2.3.1. The editorial independence of media operating on the Internet is guaranteed in law/ policy and in practice. They are not subjected to pressure to include or exclude information from their reporting or to follow a particular editorial direction.

2.3.2. Media and new media actors, including blogging websites are not required to obtain permission or a licence from the government or state authorities which goes beyond business registration in order to be allowed to operate on the Internet or blog.

2.3.3. Journalists and other media actors using the Internet are not subject to threats or harassment by the State. They do not practice self-censorship because of fear of punishment, harassment or attack.

2.3.4. The confidentiality of journalists and other media actors' sources is protected in law and respected in practice.

2.3.5. Media websites as well as websites of new media actors are not affected by cyber- attacks or other action disrupting their functioning (e.g. denial of service attacks).

2.3.6. There are prompt and effective investigations on crimes against journalists and new media actors. There is no climate of impunity.

2.3.7. Internet traffic relating to press, radio, broadcasters or any other media content is treated equally and without discrimination. Internet traffic management measures which negatively affect such content are transparent, necessary and proportionate to achieve overriding public interests in compliance with Article 10 of the ECHR.

2.4. Legality, legitimacy and proportionality of restrictions

2.4.1. Any restriction of the right to freedom of expression on the Internet is in compliance with the requirements of Article 10 of the ECHR, as interpreted by the ECtHR, namely:

- is prescribed by law, which is accessible, clear, unambiguous and sufficiently precise to enable individuals to regulate their conduct. The law ensures tight control over the scope of the restriction and effective judicial review to prevent any abuse of power. The law indicates with sufficient clarity the scope of discretion conferred on public authorities with regard to the implementation of restrictions and the manner of exercise of this discretion.

- pursues a legitimate aim as exhaustively enumerated in Article 10 of the ECHR;

- is necessary in a democratic society and proportionate to the legitimate aim. There is a pressing social need for the restriction, which is taken on the basis of a decision by a court or an independent administrative body that is subject to judicial review. The decision should be targeted and specific. Also, it should be based on an assessment of the effectiveness of the restriction and risks of over-blocking. This assessment should determine whether the restriction may lead to disproportionate banning of access to Internet content or to specific types of content and whether it is the least restrictive means available to achieve the stated legitimate aim.

2.4.2. The State does not impose undue restrictions to freedom of expression on the Internet by means of law. Defamation laws are specific and narrowly defined as to their scope of application. They do not inhibit public debate or criticism of State bodies and do not impose excessive fines or disproportionate awards of damages or legal costs. Severe sanctions, such as imprisonment, are applied only when the fundamental rights of other people have been seriously impaired such as in cases of incitement to violence or hatred.

2.4.3. Laws addressing hate speech or protecting public order, public morals, national security or official secrecy and data protection laws are not applied in a manner which inhibits public

debate about issues of public concern. Such laws impose restrictions of freedom of expression only in response to a pressing matter of public interest, are defined as narrowly as possible to meet the public interest and include proportionate sanctions.

3. The right to freedom of peaceful assembly and association

3.1. Individuals are free to use Internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards.

3.2. Associations are free to use the Internet in order to exercise their right to freedom of expression and to participate in matters of political and public debate.

3.3. Individuals are free to use Internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly.

3.3. State measures applied in the context of the exercise of the right to peaceful assembly which amount to a blocking or restriction of Internet platforms, such as social media and other ICTs, comply with Article 11 of the ECHR.

3.4. Any restriction on the exercise of the right to freedom of peaceful assembly and right to freedom of association with regard to the Internet is in compliance with Article 11 of the ECHR, namely:

- is prescribed by law, which is accessible, clear, unambiguous and sufficiently precise to enable individuals to regulate their conduct;
- pursues a legitimate aim as exhaustively enumerated in Article 11 ECHR;
- is necessary in a democratic society and proportionate to the legitimate aim. There is a pressing social need for the restriction. There is a fair balance between the exercise of the right to freedom of assembly and freedom of association and the interests of the society as a whole. If a less intrusive measure is capable of achieving the same goal the least restrictive measure is applied. The restriction is narrowly construed and applied and does not encroach on the essence of the right to freedom of assembly and association.

4. The right to private life

4.1. Personal data protection

4.1.1. The right to private life is guaranteed in compliance with Article 8 of the ECHR as interpreted by the ECtHR. Any restriction to this right pursues one of the legitimate aims exhaustively enumerated in Article 8 of the ECHR, is necessary in a democratic society and proportionate to the legitimate aim pursued.

4.1.2. The law guarantees that all personal data is protected in compliance with Article 8 of the ECHR as interpreted by the ECtHR and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) in States which have ratified it.

4.1.3. Personal data are processed lawfully (with the unambiguous consent of the data subject or on the basis of law) for legitimate purposes and not in excess of such purposes, accurately and securely. These conditions apply also to profiling (personal data automatic processing techniques that collect and use information about an individual in order to identify, analyse or predict his or her personal preferences, behaviour and attitudes).

4.1.4. Individuals are not subjected to a decision significantly affecting them based solely on automated processing of data without having their views taken into account. There are effective processes for every individual to obtain, on request, information on the processing of his or her personal data, the reason underlying processing; to object to processing; to obtain, on request, rectification or erasure of the personal data; and to consent to, object to or withdraw consent to personal data processing or profiling. Individuals have an effective remedy if these rights are not complied with. There are adequate safeguards for access to information and freedom of expression in the context of application of personal data protection legal frameworks.

4.1.5. The law defines the duties of public and private entities with regard to processing of personal data.

4.1.6. A supervisory authority, which acts with complete independence and impartiality, ensures compliance with data protection legal frameworks.

4.1.7. The State does not prohibit in law and in practice anonymity, pseudonymity and confidentiality of communications or the usage of encryption technologies. Interference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 of the ECHR.

4.2. Freedom from surveillance

4.2.1. Surveillance measures taken by public authorities (such as security services) comply with the requirements of Article 8 the ECHR and are subject to an effective, independent and impartial oversight.

4.2.2. Surveillance measures are carried out in accordance with the law, which is accessible, clear, precise and foreseeable. The law contains safeguards for the exercise of discretion by public authorities and thus defines with sufficient clarity and precision:

- the nature of offences which may give rise to surveillance measures;
- the competent authorities by which surveillance measures are carried out, the scope of any discretion conferred on such authorities and the manner of its exercise having regard to the legitimate aim of the measure in question;
- the categories of individuals liable to be subjected to surveillance measures;
- time limitations for carrying out surveillance measures;
- the procedures for examining, using and storing data obtained from surveillance measures;

- the precautions to be taken when communicating data acquired through surveillance measures to other parties and the measures applicable during the communication to ensure data security;

- the circumstances for the destruction and erasure of data obtained from surveillance measures;

- the bodies responsible for overseeing surveillance measures.

4.2.3. Surveillance measures pursue a legitimate aim as exhaustively enumerated in Article 8 of the ECHR, are necessary in a democratic society and proportionate to the legitimate aim pursued.

4.2.4. Surveillance measures carried out by State authorities either directly or through/in collaboration with private sector entities are authorised by an independent and impartial tribunal established by law or another State body who is independent from the authorities carrying out such measures and the executive.

4.2.5. Surveillance measures carried out by State authorities either directly or through/in collaboration with private sector entities do not involve activities which weaken encryption systems and the integrity of communications' infrastructure (for example built-in flaws and backdoors in security, information and communications systems).

4.2.6. Surveillance measures are subject to an effective review assured by a judicial authority or oversight by another state body offering the best guarantees of impartiality and independence from the authorities carrying out surveillance or the executive.

4.2.7. The law guarantees the right of an oversight body to have access to all information which is relevant to the fulfilment of its mandate, regardless of the level of information classification. Access to information by an oversight body extends to all relevant information held by public authorities including information provided by foreign bodies.

4.2.8. Oversight bodies exercise their powers, including seeking and handling classified information and personal data, professionally and strictly for the purposes for which they are conferred by law while ensuring that the information is protected from being used or disclosed for any purpose that is outside the mandate of such bodies.

4.2.9. Oversight bodies scrutinise the human rights compliance of surveillance measures taken by public authorities, including those taken in co-operation with foreign bodies through exchange of information or joint operations.

4.2.10. Judicial authorities and oversight bodies have the power to quash and discontinue surveillance measures undertaken when such measures are deemed to have been unlawful, as well as the power to require the deletion of any information obtained from the use of such measures.

4.2.11. Public authorities which carry out surveillance measures and their oversight bodies are not exempt from the ambit of freedom of information legislation. Decisions not to provide information are taken on a case-by-case basis, properly justified and subject to the

supervision of an independent information/data commissioner. Oversight bodies make public informative versions of their periodic and investigation reports.

5. Remedies

5.1. The State ensures that individuals have access to judicial or administrative procedures that can impartially decide on their claims concerning violations of human rights online in compliance with Article 6 of the ECHR.

5.2. The State provides for the right to an effective remedy in compliance with Article 13 of the ECHR. This includes effective non-judicial mechanisms, administrative or other means for seeking remedy such as through national human rights institutions. There are no legal, procedural, financial or other practical barriers that individuals encounter in seeking an effective remedy.

5.3. The State takes appropriate steps to protect against human rights abuses with regard to the Internet by private sector actors and to ensure that when such abuses occur within its territory and/or jurisdiction those affected have access to an effective remedy.

5.4. The States implements policies and measures to promote that all private sector actors respect human rights with regard to the Internet throughout their operations, in particular by establishing effective complaint mechanisms to address early and to remedy directly grievances of individuals whose human rights and fundamental freedoms on the Internet may be adversely impacted. Such mechanisms are legitimate (enabling trust, accountable for the fair conduct of grievances processes), accessible (known by those concerned, without barriers to access) predictable (providing a clear and known procedure with an indicative time frame for each stage, and clarity of types of processes and outcome available and means of monitoring implementation) equitable (reasonable access to sources of information, advice and expertise necessary to engage in a complaint process) transparent (keeping parties informed about the progress of a complaint) and compatible with Article 13 of the ECHR.

Appendix 4

Draft report on freedom of assembly and association on the Internet[3]

Contents

[3] *As contained in document MSI-INT (2014)08 rev5, dated 30 September 2015*

I - Introduction – Freedom of Peaceful Assembly and Association in the context of international law

1. The right to freedom of peaceful assembly and association is both a human right itself and an enabler of citizens' political participation in democratic governance. This right is also key to the achievement of economic, social and cultural rights. The right to freedom of peaceful assembly and association is enshrined in the main universal legal instruments for the protection of civil and political rights, namely, in Article 20 of the Universal Declaration on Human Rights (UDHR) and Articles 21 and 22 (respectively) of the International Covenant on Civil and Political Rights. At European level, it is protected by Article 11 of the European Convention on Human Rights (ECHR) and developed by a rich case-law of the European Court of Human Rights (ECtHR).

2. Although these provisions of international human rights law do not make any reference to the Internet or to any other medium, they provide the proper framework to guarantee the right to freedom of peaceful assembly and association for everyone independently of the technology used. The ECHR applies both to the physical world and to the online environments. The General Assembly of the United Nations has affirmed in its resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 that the same rights that people have offline must also be protected online.[4] There is an increasing number of recommendations, resolutions, declarations and reports both at the United Nations (UN) and at the Council of Europe (CoE) level that stress the importance of new technologies for their exercise.

3. Resolutions 21/16[5] and 24/5[6] of the Human Rights Council on "The rights to freedom of peaceful assembly and of association" reiterate the important role of new information and communications technologies in enabling and facilitating the enjoyment of the rights to freedom of peaceful assembly and of association.

4. The Committee of Ministers of the Council of Europe on its Recommendation to member states on a Guide to human rights for Internet users devotes an entire section to assembly, association and participation.[7] The Committee of Ministers also approved a Declaration on 7 December 2011 on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers.

5. This report studies the implications of the information telecommunication technologies (ICTs), notably the Internet, regarding the exercise and enjoyment of the right to freedom of peaceful assembly and association. It focuses in particular on the new challenges to this right and explores possible responses to them.

[4] In his 2012 Report (A/HRC/20/27), the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, called upon States "to recognize that the rights to freedom of peaceful assembly and of association can be exercised through new technologies, including through the Internet".

[5] A/HRC/RES/21/16.

[6] A/HRC/RES/24/5.

[7] CM/Rec(2014)6. This recommendation states that everyone has "the right to peacefully assemble and associate with others using the Internet. In practice, this means:

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

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

II- The Internet: The public sphere of the 21st century

1. The Internet as a tool for assembly and association

6. The ECtHR has stated in its case-law that the terms assembly and association in the ECHR have an autonomous meaning independent from their regulation in national law.[8] The ECtHR refers to an assembly as "the gathering of an indeterminate number of persons with the identifiable intention of being part of the communicative process".[9] The ECtRH has also clarified that "freedom of assembly covers both private meetings and meetings on public thoroughfares, as well as static meetings and public processions; this right can be exercised both by individual participants and by those organising the assembly".[10]

7. Regarding associations, the ECtHR has stated the "[t]he ability to establish a legal entity in order to act collectively in a field of mutual interest is one of the most important aspects of freedom of association".[11] Although only one type of association (i.e. trade unions) is expressly mentioned in Article 11 ECHR, and a relevant part of the case-law refers to political parties, the term associations is not limited to identifying those. Therefore, the term association has a broader meaning because "associations formed for other purposes, including those protecting cultural or spiritual heritage, pursuing various socio-economic aims, proclaiming or teaching religion, seeking an ethnic identity or asserting a minority consciousness, are also important to the proper functioning of democracy. […] It is only natural that, where a civil society functions in a healthy manner, the participation of citizens in the democratic process is to a large extent achieved through belonging to associations in which they may integrate with each other and pursue common objectives collectively."[12]

8. These definitions will apply also when Internet is used as a tool for assemblies or associations, although the ECtHR has not yet had the opportunity to pronounce itself on a case where its use was relevant for the decision about a possible violation of these rights. Nevertheless, there is no doubt of the ever-growing use of the Internet for such activities and the deep impact it has on how these rights are exercised.

9. There are currently around 3 billion Internet users in the world.[13] Almost two-thirds of the EU's population used the Internet daily in 2014.[14] Because of its main characteristics (namely world-wide reach, low-cost barriers to infrastructure entry and speed of communication), the Internet offers advantages to those who wish to use it as tool for assembly and association.[15]

---

[8] See *Chassagnou and others v. France*, 29 April 1999, apps. nos. 25088/94, 28331/95 and 28443/95, p. 100.
[9] See *Tatár and Fáber v. Hungary*, 12 June 2012, app. no. 26005/08 and 26160/08, p. 38. As it will be argued in this paper the nature of "the communicative process" is changing because of the Internet.
[10] See *Sergey Kuznetsov v. Russia*, 23 October 2008, app. no. 10877/04, p. 35. The European Commission of Human Rights had already stated in its inadmissibility decision on 27 October 1997 in *Anderson and others v. the United Kingdom*, app. no. 33689/96 that "The right to freedom of assembly is one of the foundations of a democratic society and should not be interpreted restrictively (No. 13079/87, Dec. 6.3.89, D.R. 60 p. 256, at p. 263). The right is applicable to private meetings and to meetings in public thoroughfares (No. 8191/78 Dec. 10.10.79, D.R. 17 p. 119), marches (No. 8440/78 Dec. 16.7.80, D.R. 21 p. 148) and sit-ins (No. 13079/87, Dec. 6.3.89, D.R. 60 p. 263). There is, however, no indication in the above case-law that freedom of assembly is intended to guarantee a right to pass and re-pass in public places, or to assemble for purely social purposes anywhere one wishes."
[11] See *Gorzelik and others v. Poland*, 17 February 2004, app. no. 44158/98, p. 88.
[12] *Idem*. p. 92.
[13] International Telecommunication Union, "The World in 2014: ICT Facts and Figures".
[14] Eurostat "Statistics in focus. Internet and cloud services - statistics on the use by individuals".
[15] The use of this kind of technologies also raises some criticism in the sense that it can become a source of "slacktivism". A definition of this term can be found in the Final Report of the World Forum for Democracy 2013, "Connecting institutions and citizens in the digital age", p. 27: "Slacktivism (sometimes slactivism or slackervism) is a portmanteau of the words slacker and activism. The word is usually considered a pejorative term that describes "feel-good" measures, in support of an issue or social cause, that have little or no practical effect other than to make the person doing it take satisfaction from the feeling they have contributed."

10. Practically, a demonstration can be convened in a matter of hours without actually having to meet the other organisers (if they exist) because all communication can take place online. Similarly in the case of associations, a group of individuals with a common goal can be created and get thousands of supporters in a matter of hours through social media without having in place a structure, statutes or registering. These could be envisaged as "informal associations" with a great organisation potential for their members to reach a common objective. "Informal associations" have always existed but the Internet has facilitated their creation and outreach. The question is how the rights exercised through them could be protected in the framework of the ECHR, taking into account that the case-law of the ECtHR focuses on a more traditional form of associations and of organisation of assemblies.
11. Social media offer opportunities for gathering support and for publicity. An interesting example is the case of Oscar Morales a Colombian who started a Facebook group called "Un millón de voces contra las FARC" (One million voices against FARC). Although the initial intention of Morales was not to organise a physical demonstration the support that this Facebook group received and the demands expressed there led to demonstrations being organised in different cities with more than 10 million attendants in Colombia and 2 million abroad, just one month after the creation of the Facebook group.[16]
12. During and after a demonstration, the Internet can be used for several purposes: to publicise it (especially when it does not receive enough coverage from traditional media), to denounce the excessive use of force by the police, to share up-to-date information (for example, where to find medical help in case of violent outbreaks), to express support by the people who cannot be physically present, to ask for or offer help, to communicate with family and friends and others.
13. The Internet is also a useful tool for associating purposes; it helps to plan activities and connect people and provides international outreach. The UN Special Rapporteur on the rights to peaceful assembly and of association, Maina Kiai, stated in his 2012 Report to the Human Rights Council that association "refers, inter alia, to civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions, foundations or even *online associations as the Internet has been instrumental, for instance, in "facilitating active citizen participation in building democratic societies*" (emphasis added).[17]
14. One example is the "Let's do it!" Project, "a civic led mass movement" which started in Estonia as an initiative to clean part of the waste of the country and create awareness of the environmental problems. They decided to organise a National Clean-up Day, which proved so successful that the Project developed into an international movement, with 112 countries working together, 11 million participants, and the annual organization of a World Cleanup day. The Internet contributed significantly to the success of the project by offering more possibilities to advertise and organise it worldwide.[18]
15. 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."[19]

[16] In the words of David Kirkpatrick in his book "The Facebook Effect: The Inside Story of the Company That Is Connecting the World" (Simon and Schuster, 2011, p. 4), "The movement that began with an impassionate midnight Facebook post in one frustrated young man's bedroom led to one of the largest demonstrations ever, anywhere in the world".
[17] A/HRC/20/27, p. 13, referring also to A/62/225, p. 91.
[18] http://www.letsdoitworld.org/
[19] 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), 2015, para. 260.

16. The importance of the Internet to get people's support for a goal can be showcased in the European Citizen's Initiative, which allows EU citizens to participate directly in the development of EU policies, by calling on the European Commission to make a legislative proposal. This mechanism has a very strong digital component, first because the organisers have to register their initiative on a website where everyone will be able to consult basic information about it.[20] Secondly, the threshold for the required statements of support can be reached by collecting them online.
17. Petitions can also be channelled through private platforms; one of the most popular is Change.org.[21] The aim of this online petition platform is to facilitate the mobilisation of citizens for different political initiatives and organising advocacy campaigns, connecting people to decision makers. As of June 2015, there were more than 100 million Change.org users in 196 countries.[22]
18. Another example is "crowdsourcing" often describing a collaborative endeavour in which a call for ideas or content is made to a large number of people[23]. It does not always need to be online, but in using the Internet as its principal conduit, the practice becomes easier and acquires an expanded potentiality.[24]
19. Furthermore, different communities may be created and operated online. An example of an online community is EdgeRyders.[25] It was developed as a joint Council of Europe and European Commission project. A platform was created where mainly young people could express their opinions on a series of topics, finally they drafted a report called "Edgeryders Guide to the Future: A handbook for policy makers and managers of policy-oriented online communities". After the completion of the project, however, Edgeryders community continued to have offline meetings but most of its work develops through a free and open source online community platform.[26]
20. The Internet and other ICTs can also facilitate protests. An example is the one against the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA), on January 18, 2012. That day 115,000 websites (including Reddit, English Wikipedia, Google, Mozilla, and Flickr) changed their main image to black explaining their disagreement with the proposed bills, three million people e-mailed Congress to voice their opposition to the bills and there were more than 2.4 million SOPA-related tweets in 16 hours.[27]
21. Another online protest occurred with the initiative "The Day we fight back", an online campaign/demonstration, or as the organisers defined it a "worldwide day of activism" against the mass surveillance of the National Security Agency of the United States. The aim was bring together a broad coalition of activist groups, companies, and online platforms on 11 February 2014.[28]

---

[20] http://ec.europa.eu/citizens-initiative/public/welcome
[21] https://www.change.org/
[22] http://blog.change.org/post/121953125809/who-are-the-100-million
[23] For a more developed definition of crowdsourcing built on a comparative study of more than other 40 definitions see Estellés-Arolas, Enrique and González-Ladrón-de-Guevara, Fernando, "Towards an integrated crowdsourcing definition", *Journal of Information Science*, April 2012, vol. 38 no. 2, pp. 189-200.
[24] The "Let's do it!" movement, mentioned previously, uses the ICTs in very different ways, one of the most remarkable is how they crowdsource information through the "waste mapping application" which enables anyone to find the trash points, upload the location and data using Google Earth software and target them for the next cleanup.
[25] Their nature is twofold, because they are also a social enterprise.
[26] https://edgeryders.eu/
[27] "Public Outcry Over Antipiracy Bills Began as Grass-Roots Grumbling":
http://www.nytimes.com/2012/01/20/technology/public-outcry-over-antipiracy-bills-began-as-grass-roots-grumbling.html?pagewanted=1&ref=technology&_r=0
"Twitter: More than 2.4 million SOPA tweets"
http://technolog-discuss.nbcnews.com/_news/2012/01/19/10190155-twitter-more-than-24-million-sopa-tweets?lite
The same day there were physical demonstrations in New York, San Francisco and Seattle.
[28] The result of this campaign was that over 24 million Americans and 13 million non-Americans saw The Day We Fight Back banner; 185,000 Americans registered to send over 555,000 emails (two each to their two Senators and

22. In some cases the Internet is used to exercise the right to freedom of expression and the right to freedom of assembly and association at the same time. For example, in the aforementioned instances tweeting against the SOPA or mass surveillance that exact day was evidently an exercise of the right to freedom of expression; but it could be considered as something else: an action towards a common aim with a protest endeavour. In the offline world the close link between these rights and freedoms was underlined very early in the system of the European Convention of Human Rights.[29]

23. A key difference between freedom of expression and that of peaceful assembly or association lies in their social components. While freedom of expression may be easily exercised individually, freedom of association and assembly carry an element of common interest or purpose, in many cases also a sense of community and sharing.[30] For example, a person may desire to join a platform to associate or show his or her support but not necessarily to express himself or herself individually in the strict sense of this word.

24. The boundaries between freedom of association and freedom of peaceful assembly online are sometimes blurred. "The intricacy with which the concepts of association and assembly are intertwined, and the difficulty in cleaving them apart perhaps suggests that these two rights need to be dealt with by means of an integrated approach which acknowledges their similarities and interdependence, and that the exercise of these rights faces the same challenges and opportunities."[31]

25. This is the selected approach of this report, although some times the problems are not identical and will be dealt with separately. In line with the case law of the ECtHR, this report considers freedom of assembly and association as closely linked to the freedom of expression. The ways they are exercised together or separately on the Internet should be considered on a case by case basis.

---

one to their Representative); 245,000 people internationally signed the necessaryandproportionate.org petition to demand privacy as a human right and another 56,000 joined petitions on causes.com and change.org; more than 420,000 persons shared the website on Facebook; #StopSpying and #StopTheNSA were trending topics on Twitter during the afternoon; and the banner, social media and at least 6,000 websites drove over 1 million unique visitors to the homepage. Although this was mainly focused on the Internet there were also 89,000 phone calls to legislators completed.
https://thedaywefightback.org/the-results/

[29] See *Rassemblement Jurassien Unité Jurassienne v. Switzerland,* 10 October 1979, app. no. 8191/78; the European Commission on Human Rights considered an allegation of Article 10 violation in relation to a ban on all political meetings in a particular municipal area "subsidiary in relation to that concerning the right of peaceful assembly. The problem of freedom of expression cannot in this case be separated from that of freedom of assembly (...) and it is primarily involved in this issue". The ECtHR considered in *Ezelin v. France,* 26 April 1991, app. no. 11800/85, p. 35 that "In the circumstances of the case, this provision [article 10] is to be regarded as a lex generalis in relation to Article 11, a lex specialis, so that it is unnecessary to take it into consideration separately." In *Öllinger v. Austria,* 29 June 2006, app. no. 76900/01, p. 38, the ECtHR stated that "Notwithstanding its autonomous role and particular sphere of application, Article 11 must also be considered in the light of Article 10. The protection of opinions and the freedom to express them is one of the objectives of freedom of assembly and association enshrined in Article 11".

[30] See Rainey, Bernadette, Wicks, Elizabeth and Ovey, Clare, "Jacobs, White and Ovey: the European Convention on Human Rights", Oxford University Press, 6th ed., 2014, p. 466, "The distinction between freedom of expression and freedom of assembly is found in the attempt of persuasion in a public contest." or Grabenwarter, Christoph, "European Convention on Human Rights. Commentary", C.H. Beck Hart Nomos Helbing Lichtenhahn Verlag, 2014, p. 298, "The freedom of assembly as guaranteed by Article 11 is closely connected to the freedoms enshrined in Article 10. (…) Its particular emphasis however, lays on protecting the collective expression of an opinion which is possibly more powerful, but also has a stronger impact on the opinions of others. The collectivity of the expression of opinion is a decisive criterion to distinguish the freedom of assembly from other forms of expression".

[31] Comninos, Alex, "Freedom of peaceful assembly and freedom of association and the Internet", APC Issue Paper, 2012, page 9.

2. The use of the Internet in the context of urban violence, incitement to violence and terrorism

26. ICTs as any other technology can be used in negative ways which threaten individuals or the society. An example is the riots that took place in London in 2011 where BlackBerry phones were used extensively "to communicate, share information and plan in advance the riots."[32] Nevertheless, in this context, it is also important to take into account "the potential of new technologies as a tool for anticipating and preventing violence, gathering evidence and ensuring accountability of instigators and perpetrators of violence"[33].
27. The Internet can be used to spread hate-speech, or incite to violence. The Internet and other ICTs can be used by terrorist groups to communicate their ideologies, to offer instructions on their activities, for recruitment purposes or to broadcast images in order to instil fear in worldwide audiences. For example, a study from the Brookings Institution estimated that from September to December 2014 at least 46,000 Twitter accounts were used by supporters of Da'esh, a terrorist group which refers to itself as "Islamic State", although not all of them were active at the same time.[34] It is important to find effective ways to fight against such uses of the Internet. Forms of expression relating to such activities fall outside of the protection of the European Convention on Human Rights. The European Court of Human Rights considers hate speech under Article 17 of the Convention.[35]
28. The Committee of Experts on Terrorism (CODEXTER) of the Council of Europe established as one of its priorities for 2014-2015 the fight against radicalisation, foreign terrorist fighters, and the receiving of training for terrorism, including via the Internet. It is extremely important and urgent to fight terrorists online as well as offline, and to co-operate with the social media businesses to do so, while upholding the respect for human rights.
29. On 19 May 2015, the Committee of Ministers adopted an Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, the first set of legally-binding international standards to help tackle so-called "foreign terrorist fighters". The Protocol requires countries to outlaw various actions including intentionally taking part in terrorist groups, receiving terrorism training or travelling abroad for the purpose of terrorism; actions that in many cases are facilitated by the Internet. The Committee of Ministers also

[32] The Guardian and London School of Economics "Reading the Riots: Investigating England's summer of disorder", p. 4. http://www.theguardian.com/uk/interactive/2011/dec/14/reading-the-riots-investigating-england-s-summer-of-disorder-full-report To add a positive note on the use of social media to organize and associate people for a good community goal, it can be recalled that Facebook and Twitter were used after the riots to mobilise hundreds of people to clear debris from streets in London's worst-hit communities. The Guardian, "London riots: hundreds answer appeal to clean up streets"
http://www.theguardian.com/uk/2011/aug/09/london-riots-cleanup-appeal
[33] Resolution on Responses of justice to urban violence of the 31st Council of Europe Conference of Ministers of Justice (Vienna, 2012), p. 16. In his Statement to the Conference, Nils Muižnieks, Council of Europe Commissioner for Human Rights, stressed that: "In some instances, social networks have played an instrumental role in the practical organisation of urban violence. The criminal justice system must obviously respond to the new challenges that this implies. But in adapting their response, States should be extra cautious not to curtail fundamental freedoms, notably freedom of expression and assembly, which are increasingly exercised through the Internet. (…) Proportionality and judicial oversight appear as two particular key principles that should be systematically applied"
[34] Berger, J.M. and Morgan, Jonathon, "The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter", Brookings Paper, March 2015.
[35] "[T]here is no doubt that any remark directed against the Convention's underlying values would be removed from the protection of Article 10 [freedom of expression] by Article 17 [prohibition of abuse of rights] (…)" (ECtHR decision on the admissibility, *Seurot v. France*, 18 May 2004, no 57383/00). See also Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

adopted that day a political declaration[36] and a three-year action plan on the fight against violent extremism and radicalisation leading to terrorism which sets out a series of Council of Europe-led measures to help tackle them, inter alia, on the Internet.

30. Measures taken by State authorities or in co-operation with Internet service or platform providers to address content and behaviour that is apologetic of terrorism must be necessary for and proportionate to the legitimate aim that they pursue, in compliance with Article 10 of the ECHR. The legislative frameworks on the basis of which such measures are taken should balance the protection of Internet users' freedom of expression, association and peaceful assembly, with legitimate social imperatives such as prevention of crime and disorder.

31. These measures should not be used to quash mere political dissent and their impact on freedom of peaceful assembly and association should be studied in order not to apply the measures too broadly, for example, blocking legitimate content. It should be noted that the ECtHR has made clear that the protection of 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 the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society". (…) From another standpoint, whoever exercises his freedom of expression undertakes "duties and responsibilities" the scope of which depends on his situation and the technical means he or she uses."[37]

32. It is also important to mention other alternative methods to fight against hate-speech and extremism online. For example, the Council of Europe has developed an extensive campaign with a widespread network of partners to fight against Hate Speech, the No Hate Speech Movement, which tries to improve awareness-raising and empower users.[38] There is also an effort to create counter-narratives that people can find easily online.

III - Challenges and questions related to the exercise and enjoyment of freedom of peaceful assembly and association online

1. Legal frameworks

33. Most of the European countries currently protect peaceful assemblies organised via social media in the same way as other assemblies.[39] One of the challenges ensuring full protection lies in having clear guidance and protocols for the law-enforcement authorities with regard to non-physical gatherings which happen entirely online or physical assemblies which are convened through online tools. These gatherings may differ from traditional assemblies in terms of their absence of an organiser, spontaneity, speed of development, or unforeseeable numbers of participants.

[36] In this Declaration, the Ministers express their intention to "encourage initiatives to combat radicalisation and the recruitment of terrorists online, in co-operation with the media and new communication services and while respecting their independence and freedom of expression. In this context, we [the Ministers] support the development of counter-narratives to extremist messages. We [the Ministers] also call for the signature and ratification of the relevant Council of Europe legal instruments by the largest possible number of States in order to better combat the transfrontier dimension of hate speech disseminated through the internet."

[37] Judgment of the ECtHR, *Handyside v. the United Kingdom*, 7 December 1976, no. 5493/72, p. 49.

[38] http://www.nohatespeechmovement.org/

[39] See 'Comparative study on national legislation on freedom of peaceful assembly', Venice Commission (CDL-AD(2014)024), p. 140.

34. In many States the concept of assembly which is protected by the law requires the physical presence of several persons in a specific place at a specific time.[40] If applied strictly in the online world, this requirement would afford a peaceful online gathering solely the protection of freedom of expression. Legal requirements which would apply to a peaceful assembly in the physical world, as for example obtaining permission from authorities, informing them about the assembly or giving notice of intent to assemble, raise new questions about how to address this point in legislation protecting the right to freedom of assembly in the digital world. As stated in the Joint Guidelines on Freedom of Peaceful Assembly of the Venice Commission and the OSCE: "Prior notification should only therefore be required where its purpose is to enable the State to put in place necessary arrangements to facilitate freedom of assembly and to protect public order, public safety and the rights and freedoms of others".[41]

35. Traditionally, in order to organise a demonstration, a well-established structure was necessary to build support, organise and coordinate such demonstration. In online environments these actions are rendered easier by ICTs and the Internet. Often there is no identifiable organiser. Sometimes this ambiguity is purposeful in decentralised movements which prefer to act collaboratively, where many people can have a role at different moments but where there is no leader as such. However, the missing organiser could pose problems to authorities who require a legitimate interlocutor with whom they can speak about safety issues or changes of location, or continue dialogue.[42] Given such ambiguous circumstances, there needs to be further discussion regarding notification for assemblies facilitated through the Internet and ICTs.

36. The immediacy of the Internet could also affect the legal definition and application of legislation regarding spontaneous demonstrations. It is extremely easy and quick to call for an assembly via social media. Also, the speed of development in social media could result in actions different from those intended by the original call for assembly. Thus there should be additional awareness-raising about these implications to assemblies facilitated through the Internet and ICTs.

37. With regard to associations, the legislation of some states still requires that these hold meetings at which members are physically present. It is questionable whether this requirement is still feasible in the digital society. The Joint Guidelines of the Venice Commission and the ODIHR state that "legislation should ensure that an association can exist online or, at the very least, can conduct many of its activities online." [43] These activities can include, for example, registering, gathering signatures, fundraising and making donations. On the other hand the Joint Guidelines state that "persons may be associated online without their express consent and not of their own volition. Such involuntary associations or memberships should not lead to legal consequences for the persons concerned." [44] Therefore, there should be awareness of these particular aspects of association online.

38. Overall, it is important to underline that the legal frameworks on freedom of assembly and association, whenever there are questions about their application to online activities,

[40] *Ibid*, p. 146, "(t)o enjoy the constitutional protection of freedom of assembly at least two people must come together for a common purpose. "Coming together" in this context requires the physical presence of several persons in a specific place at a specific time. By contrast, the coming together of several people in the virtual world, for example in a chat room in the Internet, lacks the element of physical presence of a potentially huge number of people in the same place at the same time that gives collective manifestations a particular weight, but also creates specific risks which justify a separate constitutional guarantee".

[41] Joint Guidelines on Freedom of Peaceful Assembly of the European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), 2010, p. 17-18.

[42] Tufekci, Zeynep, "Social Movements and Governments in the Digital Age: Evaluating a Complex Landscape", *Journal of International Affairs*, Fall/Winter 2014, Vol. 68, No. 1.

[43] 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), 2015, para. 261.

[44] *Ibid*.

are interpreted in favour of the exercise and enjoyment of this freedom in compliance with Article 11 of the ECHR.

2. Restrictions of Internet access, blocking and filtering

39. Internet access is a prerequisite for exercising the right to assembly and association online. The Committee of Ministers of the Council of Europe uphold that "access to the Internet is inextricably linked to human rights".[45] Council of Europe member states should satisfy the legitimate expectation of their citizens that Internet services be accessible and affordable, secure, reliable, and ongoing.[46]

40. Some of the more pressing issues were described by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, in his report of 2011, where he expressed his concerns for "the emerging trend of timed (or "just-in-time") blocking to prevent users from accessing or disseminating information at key political moments, such as elections, times of social unrest, or anniversaries of politically or historically significant events. During such times, websites of opposition parties, independent media, and social networking platforms such as Twitter and Facebook are blocked, as witnessed in the context of recent protests across the Middle East and North African region. In Egypt, users were disconnected entirely from Internet access."[47]

41. The Internet is considered to have been a catalyst of the Arab Spring, which led to some countries blocking access to the Internet in order to avoid further demonstrations. There were instances of switch-offs in Egypt, Syria and Libya in 2011.[48] Interferences such as these with freedom of expression necessarily raise serious questions about their proportionality. They concern not only freedom of expression but also the right to freedom of association and peaceful assembly of the people concerned, because it can be inferred that their aim was to prevent people from organising themselves or assembling.[49]

42. There can be also more geographically and time limited disconnections from the Internet. For example, the officials of the Bay Area Rapid Transit (BART) shut down all cell phone service in several selected subway stations for just a few hours during August of 2011, in order to avoid violence by protesters against police brutality, as well as the disruption of traffic. This action raised some issues because "(t)his appears to be the first time American authorities blocked cell phone and Internet activity in the context of a public demonstration. The incident provoked extensive legal debate over the proper governmental reaction to "flashmobs," in view of concerns that BART's actions violated both the First Amendment and the Communications Act of 1934."[50]

---

[45] Declaration of the Council of Europe Conference of Ministers responsible for Media and Information Society (2013). "Freedom of Expression and Democracy in the Digital Age".

[46] Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet.

[47] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27), p. 30.

[48] See "Egypt's big internet disconnect" http://www.theguardian.com/commentisfree/2011/jan/31/egypt-internet-uncensored-cutoff-disconnect, "The truth about Twitter, Facebook and the uprisings in the Arab world" http://www.theguardian.com/world/2011/feb/25/twitter-facebook-uprisings-arab-libya

[49] This has led to the development of new technologies that allow people to communicate with their phones even in case of switch-offs. Thanks to "mesh networking" people can communicate through a decentralised network that uses wifi or bluetooth to connect without resorting to the internet or the phone coverage, one example is the use of the Firechat app during the "umbrella-revolution" in Hong Kong. "FireChat in Hong Kong: How an app tapped its way into the protests" http://edition.cnn.com/2014/10/16/tech/mobile/tomorrow-transformed-firechat/

[50] 'Comparative study on national legislation on freedom of peaceful assembly', Venice Commission (CDL-AD(2014)024), p. 112.

43. Blocking of websites or entire Internet platforms and filtering of content may also interfere with freedom of peaceful assembly and association.[51] The European Court of Human Rights has considered the wholesale blocking of Google Sites as a violation of freedom of expression because by rendering large quantities of information inaccessible, it substantially restricted the rights of Internet users and had a significant collateral effect. [52]
44. Blocking can be also carried out autonomously by businesses. A reported example is the one of Telus, a telecom company which blocked customers' access to websites critical of Telus during a Telecommunications Workers Union strike against it.[53] Social media may also take-down or remove content. EDRi underlines that "Facebook's views on what is permissible are far from predictable. For example, in 2013, it was the company's policy to permit the uploading of videos of people being beheaded while banning pictures of breastfeeding mothers."[54] Blocking or filtering content interferes with access to the Internet, which are important as more and more people use social media and the Internet to organise themselves, associate, and assemble.
45. Pursuant to the UN Guiding principles on business and human rights state "business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."[55] In this case it means that businesses or other private entities should take into account what impact their blocking or filtering actions will have on the rights to freedom of expression, association and peaceful assembly.[56]

3. Prosecution for online activities

46. The Council of Europe's Commissioner for Human Rights (the Commissioner) has shown concern for the worrying trend of targeting of social media users who call for or organise protests though the Internet.[57] For example, the Commissioner was concerned about the climate of fear of reprisals for non-violent involvement during the Gezi Park protests, reinforced by a number of administrative and legislative measures taken during and after

[51] The Commissioner for Human Rights of the Council of Europe following the blockage of Twitter and Youtube in Turkey commended the lift of such measures by the Constitutional Court of this State, and considered that, although illegal content could be blocked, applying this measure to entire platforms was a disproportionate response in his Intervention presenting his Annual Activity Report 2013 to the Parliamentary Assembly of the Council of Europe [Report of the Thirteenth sitting, Tuesday 8 April 2014 at 3.30 p.m. (AS (2014) CR 13)].
[52] *Ahmet Yildirim v. Turkey*, 18 December 2012, app. no. 3111/10, p. 66.
[53] Austen, Ian, "A Canadian Telecom's Labor Dispute Leads to Blocked Web Sites and Questions of Censorship", The New York Times, http://www.nytimes.com/2005/08/01/business/worldbusiness/01telus.html
[54] European Digital Rights (EDRi), "Human rights violations online", p. 12. There have been critics for example coming from associations of breastfeeding mothers and cancer victims which made Facebook modify its policy of removing any kind of image which depicted nudity. The current policy of Facebook considers breastfeeding "natural and beautiful" and they "are glad to know that it's important for mothers to share their experiences with others on Facebook." The company also underlines that the vast majority of these photos are compliant with their policies. https://www.facebook.com/help/search/?query=breastfeeding
[55] First foundational principle of the Section on corporate responsibility to respect human rights of the UN Guiding Principles on Business and Human Rights.
[56] The Committee of Ministers of the Council of Europe in its Recommendation CM/Rec(2014)6 on a Guide to human rights for Internet users encouraged the private sector to engage in genuine dialogue with relevant State authorities and civil society in the exercise of their corporate social responsibility in line with these principles.
The ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, written by Shift and the Institute for Human Rights and Business and funded by the European Commission singles as an example of a possible impact in the rights of users and consumers "Government demands URL filtering and blocking systems at the national network gateway for purposes that are not in line with international human rights law (e.g. enable censorship and limit peaceful public gatherings by human right defenders)."
[57] Keynote speech by Nils Muižnieks, Council of Europe Commissioner for Human Rights to the Conference of Ministers responsible for Media and Information Society of the Council of Europe celebrated in Belgrade, 7-8 November 2013 on "Freedom of expression and democracy in the digital age- Opportunities, rights, and responsibilities".

the events. Bearing in mind the chilling effect such perceptions can have on the exercise of the rights to freedom of peaceful assembly and freedom of expression, including on the social media, he urged the Turkish authorities to discontinue any such measures already taken, and to clearly state at the highest political level that this was not a policy of the Turkish government. [58]

47. Another problem is the broad concepts that some laws have of demonstration organisers, disturbance of public order and incitement. For example, the Commissioner showed concern about a bill to amend the Spanish Criminal Code. This bill included in particular the criminalisation of the dissemination by any means of messages or orders inciting disturbance of public order or supporting the decision of disturbing public order. Although it was not clear from the wording, it has been suggested that this draft provision targeted the convocation of demonstrations through social media.[59]

48. The Commissioner considered that this reform presented the risk of limiting freedom of expression and peaceful assembly, depending on the interpretation given to the notion of 'disturbance of public order', as well as on the determination of the intention of those who allegedly incite it. He was also worried that the vague nature of this provision might in fact lead to a sanctioning of declarations and opinions expressed prior to public disturbances, which would be incompatible with international standards on freedom of expression and the case law of the European Court of Human Rights.[60]

4. Mass Surveillance

49. Another challenge to freedom of association and assembly online is mass surveillance or other interferences with privacy in the context of law enforcement and national security. Martin Scheinin, former UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, explained that:

> *"The rights to freedom of association and assembly are also threatened by the use of surveillance. These freedoms often require private meetings and communications to allow people to organize in the face of Governments or other powerful actors. Expanded surveillance powers have sometimes led to a "function creep", when police or intelligence agencies have labelled other groups as terrorists in order to allow the use of surveillance powers which were given only for the fight against terrorism. In the United States, environmental and other peaceful protestors were placed on terrorist watch lists by the Maryland State Police before political conventions in New York and Denver. In the United Kingdom, surveillance cameras are commonly used for political protests and images kept in a database. A recent poll in the United Kingdom found that one*

[58] Report by Nils Muižnieks, Commissioner for Human Rights of the Council of Europe, following his visit to Turkey from 1 to 5 July 2013 (CommDH(2013)24), paragraph. 144.

[59] Report by Nils Muižnieks, Commissioner for Human Rights of the Council of Europe, following his visit to Spain from 3 to 7 June 2013 (CommDH(2013)18), parapraph. 130.
This bill was approved and became Organic Law 1/2015 entering into force on 1 July 2015 modifying article 559 of the Criminal Code which states that "Distribution or public dissemination, through any means, of messages or orders inciting the commission of any crime of disturbance of public order of Article 557 bis of the Criminal Code, or serving to reinforce the decision to carry them out shall be punished with a fine of three to twelve months or imprisonment from three months to a year." (unofficial translation).

[60] *Ibid.*

third of individuals were disinclined to participate in protests because of concern about their privacy."[61]

50. In 1978, the ECtHR already stated that "(d)emocratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction." Nevertheless, the ECtHR, aware of the danger, inherent in secret surveillance measures, "of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".[62]

51. The ECtHR has not ruled on a case with regard to freedom of assembly and association in the context of Internet surveillance. However, there is well-established case law of the ECtHR with regard to the right to private life and the right to freedom of expression in the context of surveillance systems through other technologies. One of the fundamental principles such case law is that the ECtHR must be satisfied that whatever system of surveillance is adopted there exist adequate and effective guarantees against abuse.[63] In this context, the ECtHR has established minimum requirements with regard to the foreseeability of laws and rule of law requirements that are necessary to be included in laws that authorise surveillance systems. Moreover, the ECtHR has formulated other minimum requirements on adequate and effective safeguards against abuse under the "necessary in a democratic society test" (independent authorisation of surveillance measures[64], independent ex-post review[65], attributes of oversight bodies, powers to access information, powers to quash surveillance measures and to delete obtained data[66], etc.) In the case of *Big Brother and others v. U.K* which is currently pending before the ECtHR, the applicants (Big Brother Watch, English PEN and Open Rights Group and an expert on surveillance techniques) argue that state measures relating to surveillance of electronic communications amount to a violation of their right to privacy under Article 8 of the ECHR.[67]

52. The widespread use of ICTs also permits the collection of personal data about the people who attend a demonstration. Concerns have been voiced about the possible use of devices like IMSI catchers[68] by police during demonstrations.[69] This would allow authorities to access communications data of all people in a particular location.[70] Consequently, questions arise about the proportionality of such untargeted measures (that also affect

[61] A/HRC/13/37, p. 36. Along these lines, the Committee of Ministers of the Council of Europe issued a Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies which indicates the chilling-effect surveillance can have on the exercise of human rights. The Issue paper on Democratic and effective oversight of national security services (2015) of the Council of Europe Commissioner for Human Rights underlines the impact of national security services' activities on the rights to freedom of expression, assembly and association. Pieter Omtzigt in his report for the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe on mass surveillance (p. 25) also stated that "Regardless of whether individuals are aware of being targets of mass surveillance, the indiscriminate interception and collection of data has important ramifications with regard to the freedoms of speech, information, and association. The knowledge that States engage in mass surveillance has a chilling effect on the exercise of these freedoms."

[62] See *Klass and Others v. Germany*, 6 September 1978, app. no 5029/71, p. 42 and 49.

[63] Ibid. p. 50.

[64] Ibid. p. 54, 56*; Kennedy v. the United Kingdom*, 18 May 2010, app. no. 26839/05, p. 167; *Dumitru Popescu v. Romania,* 26 April 2007, app. no 71525/01, p. 72, 73.

[65] See *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 28 June 2007, app. no. 62540/0085, p. 87.

[66] See *Kennedy v. the United Kingdom,* p. 166, 167.

[67] Application no. 58170/13, lodged on 4 September 2013.

[68] IMSI stands for International Mobile Subscriber Identity.

[69] "Met police using surveillance system to monitor mobile phones" http://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance

[70] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (A/HRC/23/40) p. 36.

mere passers-by) and the necessary fulfilment of previous authorisation by an independent body. The possibility that ICTs offer regarding surveillance should be always tested against the requirements of Article 8 of the ECHR.

5. Anonymity

53. Another contentious element of Internet activity is anonymity. To ensure anonymity and secrecy of communications a great number of technological solutions have been developed from VPNs (Virtual Private Networks) to the ToR project.[71]. Anonymity mechanisms and encryption may be used positively, for instance in exercising human rights within repressive or authoritarian regimes. But these same mechanisms may also be used for the commission of crimes.

54. The Committee of Ministers of the Council of Europe, in its Declaration of 28 May 2003 on freedom of communication on the Internet, states that: "(i)n order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity."

55. Anonymity can also be important for certain vulnerable groups who cannot risk being identified because of possible harassment or violent attacks (e.g. women suffering abuse, LGBT persons, etc.). They would feel more secure and able to speak freely, to associate online and to fight for their rights if they know that their identities cannot be discovered. Where support for certain groups on social media can result in negative consequences, the users should be able to decide if such affiliation information is public or not. The digital footprint created by the exercise of the right to assembly online is something unparalleled by the traditional attendance to a demonstration which usually does not leave an inherent record.

56. However, anonymity and encryption may also be used to commit crimes, such as spreading hate speech. These effects on the rights of others should not be disregarded. The ECtHR has stated that "Anonymity has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet. At the same time, the Court does not lose sight of the ease, scope and speed of the dissemination of information on the Internet, and the persistence of the information once disclosed, which may considerably aggravate the effects of unlawful speech on the Internet."[72] The individual and societal benefits of anonymity and encryption should not prevent States from taking measures and co-operating in order to trace those responsible for criminal acts.

57. To respond to the problematic concerns of encryption and anonymity, the UN rapporteur on the promotion and protection of the right to freedom of opinion and expression, David, Kaye, decided to consecrate his first report since he took office to this issue. In this Report he stated that encryption and anonymity, and the security concepts behind them, provide the privacy and security that may be essential for the exercise of the right to freedom of peaceful assembly and association, therefore restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy.[73]

---

[71] https://www.torproject.org/about/overview.html.en
In its website the ToR project explains the advantages of this initiative for human rights defenders, journalists, etc. On the other hand, it is also a powerful tool that can serve for criminal purposes, as it was the case when ToR was used to put in place the wider drug market online, the "Silk Road": Christin, Nicolas "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace", *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 213-224.

[72] See *Delfi AS v. Estonia*, 16 June 2015, app. no. 64569/09, p. 147.

[73] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (A/HRC/29/32) p. 56. The UN rapporteur also stated that "Anonymous speech has been necessary for activists and protestors, but States have regularly attempted to ban or intercept anonymous

6. Civil disobedience

58. Another controversial issue is the scope of a right to protest online. The word "hacktivism" (or "hactivism") has been coined to refer to expressions of civil disobedience online. Examples include Distributed Denial of Service attacks (DDoS), website defacement and redirection.[74] A parallelism has been proposed between sit-ins in the physical world and DDoS calling them "virtual sit-ins",[75] because both hinder free traffic temporarily to get attention and show disagreement with a certain action or policy.

59. On one hand, it can be argued that these actions could be covered by freedom of expression and peaceful assembly because "(a)n assembly should be deemed peaceful if its organizers have professed peaceful intentions and the conduct of the assembly is non-violent. The term "peaceful" should be interpreted to include conduct that may annoy or give offence, and even conduct that temporarily hinders, impedes or obstructs the activities of third parties."[76] For example, in 2006, in the *Vogel* case, the Frankfurt Higher Regional Court recognised that the attempted collective blockade of a corporate website in the context of a political event is not violence or coercion, but rather a legitimate method of influencing public opinion.[77] On the other hand, interferences with computer functioning can fall under the scope of the Convention on Cybercrime of the Council of Europe (also known as Budapest Convention).[78] Such interferences can constitute criminal actions and many of them may in fact have very negative effects on the rights to freedom of expression, peaceful assembly, association or the right to property.

60. This situation seems to beg the question whether an analytical framework is needed, which would be able to address specific elements such as intent (to protest or express political or social dissent, to get the attention of the general public and contribute to the political debate) and overall impact (causing of temporary harm as opposed to permanent negative consequences for the general public), and to put in balance all these considerations. National authorities, in particular law enforcement authorities and judges should be able to consider the different elements on a case-by-case basis.[79]

---

communications in times of protest. Such attempts to interfere with the freedom of expression unlawfully pursue an illegitimate objective of undermining the right to peaceful protest under the Universal Declaration and the International Covenant on Civil and Political Rights." p. 53.

[74] DDoS consists of an attack on a website coming from multiple points whose purpose is to slow or render inaccessible a site by overcharging its servers. For example, cyber activists identifying themselves as the Electronic Disturbance Theatre and its followers sent mass amounts of page requests to the server of the Mexican Government to support the "zapatista" cause in 1998. "Defacement" is an action that changes the visual appearance of a site or webpage normally to try to pass a message. For example, a British hacker entered about 300 websites and replaced their home pages with anti-nuclear text and imagery in 1998. When a person tries to visit one website is automatically redirected to another normally where there is a message explaining the aim of the action.

[75] See Article 19 Background paper on the "Right to Protest", 2015, p. 24, referring to Wray, Stefan, "The Electronic Disturbance Theater and Electronic Civil Disobedience, June 1998.

[76] This explanation is taken from the Joint Guidelines on Freedom of Peaceful Assembly of the European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), 2010, p. 15, built in the case-law of the ECtHR, see, for example, *Stankov and the United Macedonian Organisation Ilinden v. Bulgaria*, 2 October 2001, app. nos. 29221/95 and 29225/95.

[77] Andreas-Thomas Vogel was charged with coercion as the main official organiser of a campaign of the group Libertad which promoted a DDoS attack of the web of Lufthansa to protest against the use of its planes for the forced expulsion of asylum seekers. See Peterson, Chris "In Praise of [Some] DDoSs?" http://www.cpeterson.org/2009/07/21/in-praise-of-some-ddoss/ and Bendrath, Ralf "Frankfurt Appellate Court says online demonstration is not coercion" https://edri.org/edrigramnumber4-11demonstration/

[78] T-CY Guidance Note #5 DDOS attacks (T-CY (2013)10E Rev).

[79] Article 19 in a Background on the "Right to Protest", 2015, p. 25, reiterates "the need to consider these actions as an exercise of freedom of expression and freedom of assembly and assess restrictions on them under the three part test. Similar to civil disobedience in physical world, provisions should be made for public interest considerations of prosecutorial discretion and for adopting set of mitigating factors when considering cases."

61. In any case, the persons who decide to engage in act of civil disobedience may be punished by the law. It is important that everyone who takes part in a DDoS, for example, is aware of the potential legal consequences. To the extent that the parallelism between physical sit-ins[80] and DDoS is acceptable, an important issue would be the proportionality of the sanction.[81]

IV - Conclusions

62. Regulations of freedom of assembly and association should take into account the new possibilities introduced by ICTs facilitating the exercise of these freedoms. New laws which address the use of Internet and ICTs in the context of exercise of these freedoms should not be vague or leave a too wide margin of interpretation, should not be used to hinder mere political dissent and should not have chilling effects on the right to freedom of peaceful assembly and association. The Joint Guidelines on Freedom of Association and Freedom of Peaceful Assembly of the Venice Commission and OSCE/ODIHR provide guidance about the requirements of the ECHR with regard to freedom of assembly and association which Council of Europe member States should observe.

63. As Internet access is an enabler of freedom of assembly and association, States should continue to promote Internet accessibility. General disconnections from the Internet, for instance nation-wide ones, are difficult to reconcile with freedom of expression, the right to information, the right to assembly and association, in particular as regards their lack of proportionality.

64. In order to take full advantage of the opportunities offered by the Internet and ICTs, it is necessary to improve Internet literacy, in particular by introducing it in school curricula and informal learning. It could be also very useful to create appropriate capacity-building for associations.[82] It is important for individuals and associations to know the advantages that the use of ICTs may offer them, but they have also to be aware of their responsibilities, for example, in the field of data protection, and potential legal consequences of their actions.

65. The use of ICTs, for example, social media platforms, facilitates the exercise of freedom of assembly and association; nevertheless they can also act as gatekeepers of information and/or hinder the exercise of these freedoms. It is, therefore, necessary that the businesses concerned discharge their social responsibilities with regard to human rights in the context of the development and implementation of their policies and terms of service.

66. It is important to define more precisely the legal conditions for blocking and filtering a website, by the State and private sector actors. It is necessary to assure that any measure

[80] Physical sit-ins have been considered peaceful assemblies in the European case-law, see European Commission of Human Rights Admissibility Decision on 6 March 1989 in the case of *M.C. v. Federal Republic of Germany*, no. 13079/87 and ECtHR Admissibility Decisions on 18 March 2003, in the case of *Caroline Lucas v. the United Kingdom*, no. 39013/02. Nevertheless, the detention and conviction of the people involved was considered legitimate and proportionate in the aforementioned decisions, in the first one because they were not convicted for taking part in the demonstration but because they blocked a road and " balancing the public interest in the prevention of disorder and the interest of the applicant and the other demonstrators in choosing the particular form of a sit-in, the applicant's conviction for the criminal offence of unlawful coercion does not appear disproportionate to the aims pursued." and in the second case the Court found similarly "that the actions of the police in arresting and detaining and of the national court in convicting the applicant were proportionate to the legitimate aim pursued in view of the dangers posed by the applicant's conduct in sitting in a public road and the interest in maintaining public order as well as the relatively minor penalty that was imposed."

[81] Sauter, Molly, *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet,* Bloomsbury, 2014, p. 142. Sit-ins in the United States "would typically result in charges of trespass, if anything" while the people who take part in a DDoS could result in prison charges and be condemned to pay a high fine.

[82] One example is the Guidebook on social media and youth participation by Karima Rhanem with the support of Ramsey George in the framework of the Partnership between the European Commission and the Council of Europe in the field of youth: http://pjp-eu.coe.int/documents/1017981/1668209/Social+Media+youth+participation_2013.pdf/6aa795c2-b9c8-485c-b6f7-f4175aed64a5

taken follows the conditions for a legitimate interference as stated in Article 10.2 and 11.2 of the European Convention on Human Rights.

67. The effective exercise of the duties of law-enforcement agents is basic for the protection of public security and order. Nonetheless, new surveillance possibilities that ICTs bring should always be exploited ensuring the respect of Articles 8, 10 and 11 of the ECHR.

68. The roles of anonymity and encryption should also be reflected upon (especially intention and impact), to acknowledge their value for the meaningful exercise of human rights while still protecting the rights of others that may be impacted.

69. National authorities, including law enforcement and judges should be aware that civil disobedience may take place on the Internet. The intent of those engaging in such online disobedience is an important element to be assessed in general context and together with other circumstances of the case.