

Draft report on freedom of assembly and association on the Internet

Contents

I - Introduction – Freedom of Peaceful Assembly and Association in the context of international law	2
II- The Internet: The public sphere of the 21st century	3
1. The Internet as tool for assembly and association	3
2. The Internet as a space for assembly and association	5
3. The distinction between freedom of expression and freedom of association and peaceful assembly online.....	7
4. The use of the Internet in the context of urban violence, incitement to violence and radicalization	8
III - Challenges to the exercise and enjoyment of freedom of peaceful assembly and association online.....	10
1. Addressing this freedom adequately in legal frameworks.....	10
2. Restrictions of Internet access, filtering and blocking	12
3. Prosecution for online activities	14
4. Mass Surveillance	15
5. Anonymity.....	18
6. Is online civil disobedience part of the right to protest?	18
IV- Possible responses to these challenges and conclusions	20

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. There is now a broad understanding and well-established international position that the right to freedom of peaceful assembly and association applies equally online as offline.¹ There is an ever-increasing number of recommendations, resolutions, declarations and reports both at the United Nations and at the Council of Europe (CoE) level that stress the importance of new technologies for their exercise.

3. Resolutions 21/16² and 24/5³ 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. They further describe the need for all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries.

4. The Committee of Ministers of the Council of Europe has also taken a similar position. Its Recommendation to member states on a Guide to human rights for Internet users devotes an entire section to assembly, association and participation.⁴ The Committee of Ministers also approved a Declaration on 7th 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.

¹ 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".

² A/HRC/RES/21/16.

³ A/HRC/RES/24/5.

⁴ CM/Rec(2014)6.

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.

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

1. The Internet as tool for assembly and association

6. There are currently around 3 billion Internet users in the world.⁵ Almost two-thirds of the EU's population used the Internet daily in 2014.⁶ 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.⁷ Practically, a demonstration can be convened in a matter of hours without actually having to meet the other organisers (if they exist) because all the communications can take place online. In particular, social media offer opportunities for gathering support and for publicity.

7. 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.⁸

⁵ International Telecommunication Union, "The World in 2014: ICT Facts and Figures".

⁶ Eurostat "Statistics in focus. Internet and cloud services - statistics on the use by individuals".

⁷ In addition, according to a Study of the Pew Research Center on the "The social side of the Internet" done in 2011, Internet users are more prone to associate in general. The study "found that 75% of all American adults are active in some kind of voluntary group or organization and internet users are more likely than others to be active: 80% of internet users participate in groups, compared with 56% of non- internet users. And social media users are even more likely to be active: 82% of social network users and 85% of Twitter users are group participants."

It is also worthy of mentioning that people fear that there is a risk that some persons only act online, which, while making them feel that they have already done something, actually inhibits them from engaging in action with real effects in the physical world. There is even a term coined for it: "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."

⁸ 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".

8. 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.

9. The Internet is also a useful tool for associating purposes; it helps to plan activities and connect people and provides international outreach. 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.⁹

10. 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."¹⁰

11. 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.¹¹ Secondly, the threshold for the required statements of support can be reached collecting them online.

⁹ <http://www.letsdoitworld.org/>

¹⁰ Joint Guidelines on Freedom of Association of the European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), 2014, § 260.

According to a Study of the Pew Research Center on the "The social side of the Internet" done in 2011, when Americans were asked to assess the overall impact of the internet on group activities large percentages of them believed that Internet had a major impact on the ability of groups to communicate with members (68%); to draw attention to an issue (62%); to connect with other groups (60%); to impact society at large (59%); to organise activities (59%); to raise money (52%); to recruit new members (51%); to impact local communities (49%); and to find people to take leadership roles (35%).

¹¹ <http://ec.europa.eu/citizens-initiative/public/welcome>

12. Petitions can also be channelled through private platforms; one of the most popular is Change.org.¹² 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. There are more than 95 million Change.org users in 196 countries.¹³

13. The Internet is a good platform for coming together to contribute to a common goal. This is the reason why, in recent years, “crowdsourcing” has become very popular. This concept can be defined as a collaborative endeavour in which a call for ideas or content is made to a large number of people,¹⁴ 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.¹⁵

14. In these last examples, Internet is a tool but it can also be seen as something else as will be explained in the next section.

2. The Internet as a space for assembly and association

15. In addition to facilitating people’s assembly and association in the physical world, the Internet can itself be envisaged as the space in which associations or assemblies take place. In this case assemblies and associations would be considered as entirely digital.

16. 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).¹⁶ A similar understanding of assembly and association is included in the CoE Guide to human rights of Internet users where the Internet is considered both as a tool and a space in which one may exercise the right to freedom of peaceful assembly and association.¹⁷

¹² <https://www.change.org/>

¹³ <http://www.letsdoitworld.org/>

¹⁴ For a more developed definition of crowdsourcing built on a comparative study of more than other 40 definitions see Enrique Estellés-Arolas and Fernando González-Ladrón-de-Guevara “Towards an integrated crowdsourcing definition”, *Journal of Information Science*, April 2012, vol. 38 no. 2, p. 189-200.

¹⁵ 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.

¹⁶ A/HRC/20/27.

¹⁷ Note 4.

17. The creation of online communities also illustrates the idea of envisaging the Internet as a space for assembly and association. An example of an online global community is EdgeRyders.¹⁸ 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 "Edgeriders Guide to the Future: A handbook for policy makers and managers of policy-oriented online communities". After the completion of the project, however, they realised that they had created a community worthy of continuation. They have offline meetings but most of their work develops through a free and open source online community platform.¹⁹

18. The Internet can be envisaged also as a space for protests. An example is the protest 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.²⁰

19. 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. Their aim was bring together a broad coalition of activist groups, companies, and online platforms on February 11th 2014. The idea was that Internet users would visit the dedicated website, sign up to indicate that they would participate and receive updates, install widgets on websites encouraging its visitors to fight back against surveillance, use the social media tools on the site to announce their participation, develop memes, etc.²¹

¹⁸ Their nature is twofold, because they are also a social enterprise.

¹⁹ <https://edgeriders.eu/>

²⁰ "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.

²¹ The result 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 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; more than 84,000 shared the thedaywefightback.org on Twitter, and #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/>

20. Although the examples given in this section are clearly using the Internet as a space for assembly or association online, sometimes the distinction with the use of it as a tool are not so obvious. The examples of petition gathering or crowdsourcing used in the previous section are in the edge and could be considered in one way or another depending on different factors or considerations.

3. The distinction between freedom of expression and freedom of association and peaceful assembly online

21. It is very difficult to differentiate between the exercise of the right to freedom of expression and the right to freedom of assembly and association online. 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.

22. Distinguishing an act of communication from an act of association or an act of assembly is easier in the physical world than in the digital world. In many cases these freedoms may be exercised at the same time and therefore it becomes necessary to consider that some acts fall under one or another or both rights. This may involve an examination from the angle of all these rights and freedoms.

23. For the purposes of this study, the definitions of the Joint Guidelines of the Venice Commission and the OSCE/ODIHR on freedom of peaceful assembly and on freedom of association, respectively, will be used:

- an assembly is "the intentional and temporary presence of a number of individuals in a public place for a common expressive purpose."

- an association is "an organized, independent, not-for-profit body based on the voluntary grouping of persons with a common interest, activity or purpose."

24. Taking these definitions into account, a key difference between freedom of expression and that of peaceful assembly or association consists 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. 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, in any case a positive act which could be more broadly considered as an "expression" would be necessary in the online world.

25. The issue is not only related to which right is being exercised (because they have very similar limits), the question is also the recognition of online association or peaceful assemblies as such, so that they can enjoy the same protection and standing that their offline equivalents receive.

26. 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 face the same challenges and opportunities."²² This is the selected approach of this study, although some times the problems are not identical and will be dealt with separately.

4. The use of the Internet in the context of urban violence, incitement to violence and radicalization

27. ICTs as any other technology can be used in negative ways which threaten other individuals and the society. An example is the riots that took place in London in 2011 where BlackBerry phones (BBM) were used extensively "to communicate, share information and plan in advance the riots."²³ 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"²⁴.

28. The Internet can be used to spread hate-speech, or incite to violence, especially worrying is the use made by terrorist to seek publicity, find supporters and indoctrinate and radicalise people through the Internet. It is important to find effective ways to fight against this abuse 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.

²² Comninos, Alex, Freedom of peaceful assembly and freedom of association and the Internet, APC Issue Paper, page 9.

²³ 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>

²⁴ Resolution on Responses of justice to urban violence of the 31st Council of Europe Conference of Ministers of Justice (Vienna, 2012), §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 particularly key principles that should be systematically applied when looking at issues such as: restricting access of specific individuals to the Internet; carrying out surveillance on their Internet activities; or punishing those who have instigated violence. Hopefully, the flexibility inherent to the concept of proportionality can accommodate present-day reality: when it comes to freedom of expression, the Internet is still a somewhat atypical space, whose undefined contours for users should warn against approaches that are too heavy-handed."

29. The use of the Internet by the terrorist group so-called "Islamic State" ("IS") of the ICTs is well known. New media enables them "to offer information, guidance, instruction and it remains their principal tool for communication and ideologically encouraging individuals to act independently if they cannot join the group in Iraq or Jordan."²⁵ A study from the Brookings Institution estimated that from September through December 2014 at least 46,000 Twitter accounts were used by IS supporters, although not all of them were active at the same time.²⁶ It is clear that their use of ICTs serves illegal associative activities, including promoting recruitment.

30. 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.

31. In January 2015, the Committee of Ministers adopted the terms of reference for the Committee on Foreign Terrorist Fighters and Related Issues (COD-CTE), it examined the criminalisation of acts like, inter alia, being recruited, or attempting to be recruited, for terrorism; receiving training, or attempting to receive training, for terrorism; that in many cases are facilitated by the Internet. In March 2015, the COD-CTE submitted the Draft Additional Protocol to the Convention on the Prevention of Terrorism to CODEXTER, which examined and adopted it in April 2015 subsequently submitting it to the Committee of Ministers for its final approval. The Parliamentary Assembly approved its opinion on 23 April 2015.

32. 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.

33. 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 them in a too-broad sense manner, for example, overblocking 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

²⁵ Gohel, M.J. and Sajjan, M., Asia Pacific Foundation Analysis – Jordan, "Daesh Escalating Tensions After Killing Jordanian Pilot", 4 February, 2015.

²⁶ Berger, J.M. and Morgan, Jonathon, "The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter", Brookings Paper, March 2015.

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."²⁷

34. It is also important to mention other alternative methods to fight against hate-speech and radicalisation online, 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.²⁸ There is also an effort to create counter-narratives that people can find easily in the net.

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

1. Addressing these freedoms adequately in legal frameworks

35. Most of the European countries have reacted and currently protect peaceful assemblies organised via social media in the same way as other assemblies.²⁹ One of the challenges ensuring full protection lies in having clear guidance and protocols for the law-enforcement authorities when facing assemblies which happen entirely online or are convened through online tools because of "their spontaneity, the missing organizer and the unforeseeable number of participants and partially, due to the missing legal framework."

36. In many States the concept of "assembly" protected by the law requires the physical presence of several persons in a specific place at a specific time.³⁰ If applied strictly in the online world, this requirement would deprive any peaceful online assembly of protection which is questionable in light of the principle that human rights should be protected online as they are offline. Depending on the nature of activity, the guarantees of the freedom of expression would probably lend protection in such cases.

²⁷ Judgment of the ECtHR, 7 December 1976, *Handyside v. The United Kingdom*, no. 5493/72, § 49

²⁸ <http://www.nohatespeechmovement.org/>

²⁹ Peters, Anne and Ley, Isabelle, "Comparative study on national legislation on freedom of peaceful assembly", requested by the Venice Commission (CDL-AD(2014)024), § 484.

³⁰ For example, in Germany, Professor Rainer Grote explains that "(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", in Peters, Anne and Ley, Isabelle, "Comparative study on national legislation on freedom of peaceful assembly", requested by the Venice Commission (CDL-AD(2014)024), § 146.

37. Other requirements which would traditionally 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 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". In many instances this would not be the case of online assemblies, because it seems to address mainly the occupation of a public place (squares and streets), the effects this occupation has on bystanders and daily events, and the need for police protection against violence by the demonstrators, including vandalism.

38. Traditionally, in order to organise a demonstration, a well-established structure was necessary to acquire support, coordinate and reach a critical mass. With ICTs, the process is simplified, as a call for protest can go viral without real reflection on how to articulate its desired action. In online environments, it is possible to encounter demonstrations which lack an identifiable organiser. Sometimes this ambiguity is purposeful as certain movements prefer to act collaboratively in a decentralised and horizontal way, where many people can have a role at different moments but where there is no leader as such.³¹ The missing organiser could pose problems to the authorities, who lack a legitimate interlocutor with whom they can speak about safety issues or changes of location, or actually negotiate (although sometimes this is also used as an excuse not to start a real dialogue). This may also weaken the long-term objectives of an association or an assembly because it is more difficult to sustain them over time.³²

39. Probably, the immediacy of the Internet should also make us rethink how we deal with or what we understand for spontaneous demonstrations, and if the time lapses for notification are still up to date. It is extremely easy to call for an assembly via social media, so there should be also awareness-raising about what the lack of this notification may suppose for the person responsible.

40. The legislation of certain states also requires that associations hold meetings at which members are physically present. It could be questioned what is the specific legitimate aim of this requirement and if it is necessary and proportionate in the current "digital society". The Venice Commission and the ODIHR consider that associations should be able to exist

³¹ 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.

³² 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.

fully online or, at the very least, to have the possibility to conduct many of their activities online.³³

2. Restrictions of Internet access, filtering and blocking

41. 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".³⁴ Council of Europe member states should satisfy the legitimate expectation of their citizens that Internet services be accessible and affordable, secure, reliable, and ongoing.³⁵

42. Some of the more pressing issues were described by the 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."³⁶

43. The Internet played a major role in the Arab Spring, which led to some countries blocking access to Internet in order to avoid further demonstrations. There were instances of switch-offs in Egypt, Syria and Libya in 2011. 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.

44. 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

³³ Joint Guidelines on Freedom of Association of the European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), 2014, § 260 and 261.

³⁴ 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".

³⁵ Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet.

³⁶ 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), § 30.

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.”³⁷

45. Blocking, filtering or take down of particular content can affect entire platforms as was the case of Twitter and YouTube blocked in Turkey during some months in 2014. The Turkish Constitutional Court deemed it illegal because it impinged upon freedom of expression. Such blocking also has an impact on freedom of association and peaceful assembly as Twitter is a tool which enables their functioning.³⁸

46. Blocking can be also carried out autonomously by businesses. A reported example is the case of Telus, a telecom company which blocked the access of its clients to a website critical to the business and which supported a strike of its workers organised by its trade-union.³⁹ Take-down or removal of content by social media is also an issue. 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.”⁴⁰ Some certainty is necessary when more and more people use these sites to organise themselves, associate, and assemble.

47. The argument whether online platforms could be considered as private property would raise the question whether there is a right to exercise freedom of peaceful assembly and association in these platforms. Although, there cannot be clear cut answers to this question guidance should be sought in the ECtHR jurisprudence and other relevant documents explained below.

48. When the Joint Guidelines on Freedom of Peaceful Assembly of the Venice Commission and OSCE/ODIHR define assemblies, they clarify that: “This definition recognizes that, although particular forms of assembly may raise specific regulatory issues, all types of peaceful assembly – both static and moving assemblies, as well as those that take place on publicly or privately owned premises or in enclosed structures – deserve protection.”

³⁷ Less, Steven, in Peters, Anne and Ley, Isabelle, “Comparative study on national legislation on freedom of peaceful assembly”, requested by the Venice Commission (CDL-AD(2014)024), § 112

³⁸ The wholesale blocking of Internet platforms has been considered by the European Court of Human Rights as a violation of freedom of expression *Yildirim v Turkey*. Judgment of the ECtHR of 18 December 2012, *Ahmet Yildirim v. Turkey*, no. 3111/10.

³⁹ Ian Austen, “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?_r=0

⁴⁰ “Human rights violations online”, Drafted by European Digital Rights (EDRi), 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>

49. More specifically when they tackle the issue of assemblies in private property they say that "(t)he state may, on occasion, have a positive obligation to ensure access to privately owned places for the purposes of assembly or expression. In the case of *Appleby and Others v. the United Kingdom* (2003), a case concerning freedom of expression in a privately owned shopping centre, the European Court of Human Rights stated that the effective exercise of freedom of expression "may require positive measures of protection, even in the sphere of relations between individuals." Freedom of assembly in privately owned spaces may be deserving of protection where the essence of the right has been breached."

3. Prosecution for online activities

50. The Commissioner for Human Rights of the Council of Europe (the Commissioner) has shown concern for the worrying trend of targeting of social media users who call for or organise protests through the Internet.⁴¹ In its Report on Freedom on the Net 2014, Freedom House denounced that "(i)n tandem with the growing number of legal measures designed to restrict online speech, more people were detained or prosecuted for their digital activities in the past year than ever before." and "(s)ocial-networking sites—the new battleground for governments seeking to quell protests and organized dissent—spurred an unprecedented volume of legal and extralegal detentions."⁴²

51. For example, social media networks played a major role in the Gezi Park protests, when a number of citizens were taken into custody for posting Twitter messages about the protests. Although most of them were afterwards released, Amnesty International reported on what was called the "Twitter case" that "(t)he defendants who sent tweets reporting police violence, or called for medical aid, face charges of inciting the public to break the law. If found guilty, they could face up to three years in prison."⁴³

52. The Commissioner was deeply concerned that the reprisals for non-violent involvement during the events would have a chilling effect 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.⁴⁴

⁴¹ 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".

⁴² Freedom House, "Freedom on the Net 2014", p. 7.

⁴³ Amnesty International Press releases of 17 April 2014 "Turkey: Gezi Park Protest Twitter trial" <http://www.amnesty.org/en/for-media/press-releases/turkey-gezi-park-protest-twitter-trial-2014-04-17>

⁴⁴ 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), § 144.

53. Another problem is the broad concepts that some laws have of demonstration organisers, disturbance of public order and incitement. For example, the Commissioner also 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, some critics suggested that this draft provision targeted the convocation of demonstrations through social media.⁴⁵

54. 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.⁴⁶

4. Mass Surveillance

55. 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 third of individuals were disinclined to participate in protests because of concern about their privacy."⁴⁷

⁴⁵ 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), §130.

⁴⁶ *Ibid.*

⁴⁷ A/HRC/13/37 - §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.

56. 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"⁴⁸.

57. In the case of *Big Brother and others v. U.K* which is currently pending before the ECtHR,⁴⁹ 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.⁵⁰ This could be a test case not only for the right to privacy, but also for freedom of association and assembly, because the applicants were using these means to organize different campaigns, and they have expressed their concern about the possibility that the security services could be interested not only in collecting information about them, but also about the people they communicate with.

58. In a similar case, the Investigatory Powers Tribunal of the United Kingdom issued a judgment on February 6th, 2015, where it ruled that "prior to the disclosures made and referred to in the Tribunal's Judgment of 5 December 2014, the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or (on the Claimants' case) Upstream, contravened Articles 8 or 10 ECHR, but now complies."⁵¹

59. The ECtHR has clearly stated in its case-law that there "are two of the requirements that flow from the expression "prescribed by law". Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a

⁴⁸ Judgment of the ECtHR of 6 September 1978, *Klass and Others v. Germany*, no 5029/71, § 42 and 49.

⁴⁹ Application no. 58170/13, lodged on 4 September 2013.

⁵⁰ To get more information on the facts and allegations see the Statement of Facts and Questions to the parties communicated on 9 January 2014.

⁵¹ Judgment of the Investigatory Powers Tribunal of the United Kingdom of 6 February 2015, *Liberty (The National Council of Civil Liberties) and Others vs. The Secretary of State for Foreign and Commonwealth Affairs and Others*, cases no. IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, and IPT/13/204/CH.

degree that is reasonable in the circumstances, the consequences which a given action may entail.”⁵²

60. Techniques such as metadata analysis of an unlimited number of persons may lead to associations of a person with certain groups against his/her will or knowledge.⁵³ It is necessary to study which negative implications could arise from these techniques for freedom of association in light of requirements on international human rights law according to which “(n)o one may be compelled to belong to an association”.⁵⁴

61. Law enforcement actions (or potential) to access communications data and catch telecommunication signals may also raise concerns. For example, if the police was concerned that a demonstration may turn violent, it could establish a mobile-restricted zone in specific/designated areas, identify the electronic devices being used and the people present. The police would have access to the communications of peaceful demonstrators who had no intention of engaging in unlawful activities or who were simply walking down the street. In other words, police officers would be able to take action with no specific suspect or threat in mind and the decision over when and where to establish the designated zones would not necessarily be subject to judicial control.

62. National legislation must stipulate that state surveillance of communications shall take place only in full compliance with Article 8 of the ECHR. Surveillance would be justified only under the most exceptional circumstances, and exclusively under the supervision of an independent judicial authority. In those circumstances, safeguards must be clearly articulated, in law, to define the nature, scope and duration of the possible measures. The law must also spell out the grounds required for ordering them, as well as the authorities responsible for authorising, carrying out and supervising them.

63. Individuals should be informed when they have been subjected to communications surveillance, and when their communications data has been accessed. Advance notification may of course jeopardise the effectiveness of the surveillance, but people should always be notified once the surveillance is complete. They must also be able to seek legal redress when they believe the powers have been abused.

64. We encounter here another problem and it is that people are free to assemble or not, and with this technology any passer-by could be considered as taking part in the demonstration.

⁵² Judgment of the ECtHR, 2 August 1984, *Malone v. The United Kingdom*, no. 8691/79, § 67.

⁵³ The importance of metadata and how its storage can affect the human rights was shown by the Judgment of the Court of Justice of the European Union of 8 April 2014, *Digital Rights Ireland Ltd and Seitlinger and Others*, Joined cases C-293/12 and C-594/12.

⁵⁴ Article 20.2 of the UDHR. Although not expressly mentioned in article 11 of the ECHR, the ECtHR has stated in its case-law that this provision implies a negative freedom of association (see Judgment of the ECtHR of 30 June 1993, *Sigurður A. Sigurjónsson v. Iceland*, no. 16130/90, § 37).

65. Any measure taken to preserve public security or fight against crime, even if it has a legitimate aim, may interfere with the freedom of expression, association or peaceful assembly and has to be prescribed by law and “necessary in a democratic society” which encompasses a proportionality test.

5. Anonymity

66. Another controversial/contentious element of Internet activity is anonymity. 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.” Obviously, this does not prevent States from taking measures and co-operating in order to trace those responsible for criminal acts.

67. Anonymity is an indispensable feature for certain vulnerable groups who cannot risk being identified because of possible harassment or violent attacks (e.g. women suffering abuse, LGBTI persons, dissidents, 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 identity cannot be discovered by other users.

68. In this sense, the support for certain groups on social media can also have negative consequences, and the users should be able to decide if this information is public or not.⁵⁵

6. Is online civil disobedience part of the right to protest?

69. Another highly debated issue is the scope of a right to protest online. The word “hacktivism” (or “hactivism”) has been coined to refer to a form of modern civil disobedience online; examples include the Distributed Denial of Service (DDoS⁵⁶), website defacement⁵⁷ and redirection⁵⁸. Its supporters make a parallelism between sit-ins and DDoS

⁵⁵ For some examples of the undesired effects of this kind of revelations, see Andrews, Lori, “The Constitution in the age of Facebook: Freedom of Association”, <http://blog.constitutioncenter.org/2012/01/the-constitution-in-the-age-of-facebook-freedom-of-association/> In this article the author explains that the Federal Trade Association of the United States used a federal statute to charge Facebook with “unfair trade practices” when in 2009 the company changed its policy without any notice, so that lists of friends and affiliations were made public and no longer subject to people’s privacy controls. According to the settlement of the case, Facebook is not allowed to change its privacy settings without letting people know in advance and giving them a choice about what information they will reveal.

⁵⁶ Distributed Denial of Service 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.

⁵⁷ “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.

⁵⁸ When a person tries to visit one website is automatically redirected to another normally where there is a

calling them “virtual sit-ins”, because both hinder free traffic temporarily to get attention and show disagreement with a certain action or policy.

70. On one hand, it can be argued that these actions should be covered by freedom of expression and peaceful assembly because the Joint Guidelines on Freedom of Peaceful Assembly of the Venice Commission and the OSCE explain that “(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.”

71. 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).⁵⁹ Such interferences can constitute criminal attacks and many of them may in fact have very negative effects on the right to freedom of expression, peaceful assembly, association or the right to property.⁶⁰

72. There may be cases, however, when the objective/intent has very specific motivations, namely to express political or social dissent. These cases require a new analytical framework, which would be able to address specific elements such as the intent (motivation) and overall impact (causing of temporary harm as opposed to having permanent negative consequences for the general public) and to put in balance all these considerations.⁶¹ National authorities, in particular law enforcement authorities and judges should be able to consider the different elements on a case-by-case basis; if the aim of the act is to protest this approach should also be taken into account.

73. 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.⁶²

message explaining the aim of the action.

⁵⁹ T-CY Guidance Note #5 DDOS attacks (T-CY (2013)10E Rev). The question is what is the exact meaning of “without right” and the scope of the article 15 of the Convention.

⁶⁰ In this sense the use of these kind of tactics by States and their negative impact on human rights should also be studied, as an example the Report on Mass Surveillance of the Parliamentary Assembly of the Council of Europe § 24 describes that “The Joint Threat Research Intelligence Group (JTRIG), GCHQ’s previously secret unit, engaged in cyber-offensive missions against people who had nothing to do with terrorism or national security threats. For example, JTRIG used DDoS (Distributed Denial of Service) tactics to shut down Internet chat rooms used by members of the “hacktivist” group known as Anonymous, also affecting others using the same servers or network (a form of “collateral damage”).”

⁶¹ Molly Sauter, for example, calls for an analytical model “(r)ather than reacting based on an objection to DDOSes as a whole or comparisons to already existing activist tactic, this model looks at the motivations behind a campaign, its intended effects, its actual effects, and the technologies used before coming to a conclusion on the legitimacy of an activist action”. Sauter, Molly, “Activist DDOS: When Similes and Metaphors Fail”, HOPE9 Talk <http://oddlatters.com/2012/07/15/hope9-talk-activist-ddos-when-similes-and-metaphors-fail/>

⁶² 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

74. 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 legal consequences it may have. If we accept the parallelism between sit-ins and DDoS another issue would be the proportionality of the sanction, for example "(p)otential sentences for DDoS actions in the United States are high compared to other crimes and especially compared to other types of traditionally recognized activist activities."⁶³

IV- Possible responses to these challenges and conclusions

75. The traditional requirements and regulations of the freedom of assembly and association should take into account the new possibilities introduced by ICTs; additionally some of them have to be updated in order to adapt to the peculiarities of the cases in which these activities are partly or entirely exercised online. Safeguards for human rights should be maintained, the updating of the legislations should not be used as an excuse to further curtail human rights. New laws should not be vague or all-encompassing leaving a too wide margin of interpretation because legal certainty is of the outmost importance when dealing with the exercise of human rights.

76. As has been previously stated, Internet access is a prerequisite for exercising the right to assembly and association online. As Internet access is an enabler of freedom of assembly and association, States should strive to promote an Internet that is available, accessible and affordable.⁶⁴

77. However, Internet access is not sufficient. In order to take full advantage of the tools offered by the ICTs, it is necessary to improve Internet literacy and, furthermore, that States introduce it in school curricula and informal learning. It could be also very useful to create appropriate capacity-building for associations.⁶⁵

78. There is a need of recognition at international level that disconnection from the Internet, like the switch-offs during the Arab spring, is a violation of freedom of expression, the right

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/>

⁶³ Sauter, Molly, *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*, Bloomsbury, 2014, p. 142. She explains that a sit-in in the United States "would typically result in charges of trespass, if anything" (p. 141), while the people who take part in a DDoS could result in prison charges and be condemned to pay a high fine.

⁶⁴ Report of the UN Special rapporteur on Freedom of Expression 2011.

⁶⁵ 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

to information, the right to assembly and association, because it fails to meet the criterion of proportionality of interferences with these rights.

79. It is important to define more precisely the legal conditions for blocking and filtering a website, by the State, but also by Internet Service Providers. It is necessary to assure that any measure taken follows the conditions for a legitimate interference as stated in Article 10.2 and 11.2 of the European Convention on Human Rights. The terms of service of social media or host providers, when dealing with the take-down of content, should offer legal certainty and predictability, and should not impinge in human rights. There could be special safeguards when they are used for assembly and association activities online.

80. The effective exercise of the duties of law-enforcement agents is basic for the protection of public security and order, but sometimes the possibilities of action at their disposal dealing with ICTs are not sufficiently specified. Clear frameworks and action protocols should be developed to clarify that these measures are really in line with human rights standards and how to apply them properly.

81. The role of anonymity should also be reflected upon because in some cases it can be a condition sine qua non for a real exercise of the rights of the person, while some limits following legitimate objectives may be imposed.

82. National authorities, including law enforcement and judges should be aware that civil disobedience, which is a form of the exercise of freedom of assembly and association can 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.

83. It is important to study how States can protect the freedom of assembly and association online, because the measures could be very different that when they happen in the physical world. It is also necessary to identify the roles and responsibilities of private companies (e.g. ISPs). The UN Guiding principles on business and human rights state that "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." In this case it means that these entities have to take into account what the results of their actions will have in rights like freedom of expression, association or peaceful assembly.⁶⁶

⁶⁶ 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)."

84. Although it is important to adapt legislation and practices to the use of ICTs, some reference documents not specifically drafted for online activities like the Joint Guidelines on Freedom of Association and Freedom of Peaceful Assembly of the Venice Commission and OSCE/ODIHR continue to be a good framework that State authorities should observe.