United Nations A/HRC/41/41

General Assembly

Distr.: General
17 May 2019

Original: English

Human Rights Council
Forty-first session
24 June–12 July 2019
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Rights to freedom of peaceful assembly and of association

Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*

Summary

In the present report, the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, focuses on the opportunities and challenges facing the rights to freedom of peaceful assembly and of association in the digital age. The Special Rapporteur seeks to provide guidance on how to best preserve and maximize these opportunities and address risks.

The Special Rapporteur concludes that international law protects the rights to freedom of peaceful assembly and of association, whether exercised in person, through technologies of today, or through technologies that will be invented in the future. Existing international human rights norms and principles should not only dictate State conduct, but also be the framework that guides digital technology companies' design, control and governance of digital technologies.

* Agreement was reached to publish the present report after the standard publication date owing to circumstances beyond the submitter's control.

GE.19-08114(E)
1908114

I. Introduction

1. The present report is submitted to the Human Rights Council at its forty-first session by the Special Rapporteur on the rights to freedom of peaceful assembly and of association, pursuant to Human Rights Council resolutions 15/21 and 32/32. In section II, the Special Rapporteur provides an account of some of his activities since his presentation of his report to the Human Rights Council on 18 June 2018. In sections III and IV, he addresses the exercise of the rights to freedom of peaceful assembly and of association in the digital age. The conclusions and recommendations are detailed in section V.

2. The digital age has opened new space for the enjoyment of the rights to freedom of peaceful assembly and of association. There are numerous examples across the globe which demonstrate the power of digital technology in the hands of people looking to come together to advance democracy, peace and development. However, the digital revolution has also brought a range of new risks and threats to these fundamental rights.

3. The Special Rapporteur has observed how, over the past decade, States have used technology to silence, surveil and harass dissidents, political opposition, human rights defenders, activists and protesters, and to manipulate public opinion. Governments are ordering Internet shutdowns more frequently, as well as blocking websites and platforms ahead of critical democratic moments such as elections and protests. A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world. While the role that technology can play in promoting terrorism, inciting violence and manipulating elections is a genuine and serious global concern, such threats are often used as a pretext to push back against the new digital civil society.

4. Meanwhile, dominant online platforms such as Facebook, Twitter and YouTube have become the gatekeepers to people's ability to enjoy the rights of peaceful assembly and of association, wielding enormous power over whether individuals and civil society actors can access and participate in the democratic space.

5. The opportunities and threats that digital technologies present to the exercise of freedom of assembly and of association will increase as emerging technologies – including the Internet of Things and artificial intelligence – develop and become more common. Building on reports authored by other relevant special procedure mandate holders,[1] the Special Rapporteur seeks in the present report to provide guidance on how to best preserve and maximize the opportunities that these technologies bring while addressing their risks. The present report is not intended to be exhaustive. Rather, it aims at presenting an initial overview of the most pressing challenges, which will be further addressed in future reports and communications.

6. During the drafting of the present report, the Special Rapporteur benefited from a public process of input and consultations. On November 2018, he issued a call for inputs for the report. As at the date of publication of the report, 10 submissions from civil society organizations, 2 submissions from digital technology companies and 2 submissions from governments had been received. The Special Rapporteur convened an expert meeting in Geneva on 11 and 12 October 2018. He also held regional consultations with civil society organizations in Bangkok (21 December 2018), Beirut (18 January 2019) and Mexico City (24 and 25 January 2019), in Silicon Valley, California, United States of America (27–30 January 2019), and in Nairobi (21 and 22 February 2019). He held meetings with experts in Copenhagen (6 March 2019) and convened a consultation with governments in Geneva (20 March 2019). In addition, a joint consultation with the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, was held on 18 and 19 December 2018 in Bangkok.

[1] See, for example, A/HRC/17/27, A/71/373, A/HRC/23/40 and A/HRC/38/47.

II. Activities of the Special Rapporteur

A. Country visits

7. The Special Rapporteur visited Tunisia from 17 to 28 September 2018 (see A/HRC/41/41/Add.3) and Armenia from 7 to 16 November 2018 (see A/HRC/41/41/Add.4). He thanks both Governments for their cooperation before and during the visits.

B. Communications

8. The Special Rapporteur sent a total of 130 communications to 60 States between 1 April 2018 and 25 April 2019. His observations on communications addressed to States, and the replies received, are contained in an addendum to the present report (A/HRC/41/41/Add.1).

C. Participation in various events

9. The Special Rapporteur took part in the following events, among many others:

(a) An academic visit to Brazil from 16 to 20 July 2018;

(b) The Swiss Development Cooperation conference on shrinking civic space and an enabling environment for civil society, held in Bern on 13 and 14 September 2018;

(c) The sixty-third session of the African Commission on Human and Peoples' Rights, held in Banjul from 24 to 26 October 2018, and the sixty-fourth session of the Commission, held in Sharm El Sheikh, Egypt, on 24 April 2019;

(d) The session at the Global Human Rights Defenders Summit entitled "Making our space great again: addressing shrinking space, restrictive laws and restrictions on funding – actual situation and main issues for next 20 years", which took place in Paris on 30 October 2018;

(e) The "Civic Space under Attack" conference, held at the Utrecht University Centre for Global Challenges, the Netherlands, on 21 November 2018;

(f) The Forum on Business and Human Rights, held in Geneva from 26 to 28 November 2018;

(g) The International Organization of la Francophonie event to mark the seventieth anniversary of the Universal Declaration of Human Rights, held in New York on 10 December 2018;

(h) Regional dialogues with civil society and governments from the Asia-Pacific region on the impact of restriction to civic space, freedom of opinion, expression and assembly to elections, organized by the Asian Forum for Human Rights and Development and held in Bangkok on 20 and 21 December 2018;

(i) The annual conference of Frivillighet Norge, the Norwegian association of non-governmental organizations (NGOs), with the theme "Can NGOs save democracy?", held in Oslo on 14 February 2019;

(j) The International Conference on Claiming Civic Space Together, held in Copenhagen on 4 and 5 March 2019;

(k) The 172nd session of the Inter-American Commission on Human Rights, held in Kingston from 6 to 10 May 2019.

III. The rights to freedom of peaceful assembly and of association in the digital age: international legal framework

A. State obligations

10. The rights to freedom of peaceful assembly and of association are protected in article 20 of the Universal Declaration of Human Rights and in articles 21 and 22 of the International Covenant on Civil and Political Rights. The Human Rights Council has emphasized that States have the obligation to respect and fully protect these rights online as well as offline.[2] The General Assembly has also called upon all States to "ensure that the same rights that individuals have offline, including the rights to freedom of expression, of peaceful assembly and of association, are also fully protected online, in accordance with human rights law".[3]

11. In previous reports, the mandate holder has recognized that digital technology is integral to the exercise of the rights of peaceful assembly and association.[4] Technology serves both as a means to facilitate the exercise of the rights of assembly and association offline, and as virtual spaces where the rights themselves can be actively exercised.[5] Indeed, such technologies are important tools for organizers who seek to mobilize a large group of people in a prompt and effective manner, and at little cost, and also serve as online spaces for groups of people that are marginalized by society and are confronted with restrictions when operating in physical spaces.[6] The mandate holder has called upon States to ensure that everyone can access and use the Internet to exercise these rights, and that online associations[7] and assemblies[8] are facilitated in accordance with international human rights standards. The Human Rights Council has recognized that although an assembly has generally been understood as a physical gathering of people, human rights protections, including for freedom of assembly, may apply to analogous interactions taking place online.[9]

12. While these rights are not absolute, the freedom to access and use digital technologies for the exercise of peaceful assembly and association rights should be viewed as the rule, and the limitations as the exception. The general norm should be to permit the open and free use of the Internet and other digital tools.[10] Resolution 15/21 of the Human Rights Council makes it clear that to be permissible restrictions should be "prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others".[11] Where such restrictions are made, "States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right."[12]

13. States not only have a negative obligation to abstain from unduly interfering with the rights of peaceful assembly and of association but also have a positive obligation to facilitate and protect these rights in accordance with international human rights standards.[13]

---

[2] See Human Rights Council resolution 38/7.
[3] See General Assembly resolution 73/173.
[4] See A/HRC/20/27 and A/HRC/38/34.
[5] A/HRC/29/25/Add.1, para. 53.
[6] See A/HRC/35/28.
[7] A/HRC/20/27, para. 52.
[8] A/HRC/29/25/Add.1, para. 34.
[9] See Human Rights Council resolution 38/11.
[10] A/HRC/23/39, para. 76.
[11] See Human Rights Council resolution 15/21.
[12] Human Rights Committee, general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant, para. 6.
[13] A/HRC/17/27, para. 66; and A/HRC/29/25/Add.1.

This means ensuring that the rights to freedom of peaceful assembly and of association are enjoyed by everyone, without discrimination on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status (article 2 (1) of the International Covenant on Civil and Political Rights).[14]

14. In the digital age, the positive obligation to facilitate the exercise of the rights to freedom of peaceful assembly and of association includes efforts "to bridge the digital divides, including the gender digital divide, and to enhance the use of information and communications technology, in order to promote the full enjoyment of human rights for all".[15] The obligation to protect requires that positive measures be taken to prevent actions by non-State actors, including businesses, that could unduly interfere with the rights to freedom of peaceful assembly and of association.[16]

15. Where peaceful assembly and association rights are unduly restricted, the victim(s) should be able to exercise their rights to an effective remedy and obtain redress. The Human Rights Council has called on States to "ensure effective remedies for human rights violations, including those related to the Internet, in accordance with their international obligations".[17]

16. Violations of the rights of peaceful assembly and association may also interfere with the enjoyment other human rights, both offline and online. These include the right to privacy and the right to freedom of opinion and expression, which are intimately related to the enjoyment of peaceful assembly and association rights. Other rights may also be affected, particularly economic, social and cultural rights.

B. Role and responsibilities of business

17. In the digital age, the exercise of the rights of peaceful assembly and association has become largely dependent on business enterprises, whose legal obligations, policies, technical standards, financial models and algorithms can affect these freedoms. Online platforms and social media companies, in particular, wield significant power over how both the right to freedom of peaceful assembly and the right to freedom of association are enjoyed and exercised, particularly in countries where the "offline" exercise of the rights to freedom of peaceful assembly and of association is heavily curtailed. These platforms, however, have also become new tools for targeting and surveilling civil society actors.

18. The global framework for assessing digital technology companies' responsibilities to respect human rights is provided by the Guiding Principles on Business and Human Rights.[18] Guiding principles 11–24 recognize that business "should respect human rights" by avoiding infringing on the human rights of others and by addressing adverse human rights impacts with which they are involved. In order to fulfil this obligation, business enterprises should have in place human rights policies and processes – including a policy commitment to meet their responsibility to respect human rights; a human rights due diligence process to identify, prevent, mitigate, and account for how they address, their human rights impacts; and processes to enable the remediation[19] of any adverse human rights impacts that they cause or to which they contribute.

19. In this regard, the mandate holder associates himself with the views of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and

[14] See also article 26 of the Covenant.

[15] Human Rights Council resolution 38/7, para. 5. This is also reflected in the 2030 Agenda for Sustainable Development, which contains a commitment to "significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020" (target 9.C) and to "enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women" (target 5.B). See also A/HRC/35/9.

[16] See article 2 (2) of the Covenant; and Human Rights Committee, general comment No. 31.

[17] See Human Rights Council resolution 38/7.

[18] A/HRC/17/31.

[19] A/72/162, para. 86 (c).

expression, who has indicated that "human rights law gives companies the tools to articulate and develop policies and processes that respect democratic norms and counter authoritarian demands".[20] Similarly, the Human Rights Council has recognized that "international human rights law should guide private sector actors and be the basis for their policies".[21]

20. States, for their part, have obligations to protect human rights and prevent violations in relation to the actions or inaction of third parties such as businesses. Guiding principle 1 affirms that "States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication."[22]

IV. Exercise of the rights to peaceful assembly and association in the digital age: opportunities and challenges

A. Digital opportunities

21. Digital technologies have brought remarkable opportunities for the enjoyment of the rights of freedom of peaceful assembly and of association. By serving both as tools through which these rights can be exercised "offline" and as spaces where individuals can actively form online assemblies and associations,[23] digital technologies have vastly expanded the capacities of individuals and civil society groups to organize and mobilize, to advance human rights and to innovate for social change.

22. The role of social media in mobilizing people to the streets is well known. During his visit to Armenia in 2018, for instance, the Special Rapporteur heard several stories of how social media platforms, live-streaming tools and communication apps had played a key role in the "velvet" revolution of 2018 that had led to the resignation of the Prime Minister. The hashtags #MyStep and #MerzhirSerzhin had been used to share information, and mobilize citizens and gather their support, circumventing the government-controlled media. The #BlackLivesMatter movement for racial equality began with the use of a hashtag to mobilize communities in mass protests in the United States and other parts of the world against police violence and systemic racism towards people of African descent. Many youth movements across the world are supported by social media, as demonstrated by the #RoadSafetyMovement in Bangladesh, the #FeesMustFall campaign in South Africa, and the #FridaysForFuture and #ClimateStrikes global movement.

23. Individuals can now use online spaces to participate in a virtually connected civil society. Women activists, for example, use the Internet to connect and to exchange strategies, including across borders, and as a space for organizing.[24] The #MeToo movement is perhaps the most notable recent example. In 2017, survivors of sexual violence used social media platforms to share personal stories of sexual harassment and abuse and to call for gender equality in the workplace, under the hashtag #MeToo. Within a year, the hashtag had reportedly been used more than 19 million times[25] both by survivors and by supporters of the cause. Although the movement began in the United States, women also joined in France (#BalanceTonPorc), in the Arab world (#AnaKaman), in India (#MeTooIndia), in Ukraine (#IAmNotAfraidToSayIt) and in Mexico (#MeTooMexico) also joined.

[20] See A/HRC/38/35.
[21] See Human Rights Council resolution 38/7.
[22] See A/HRC/17/31.
[23] See A/HRC/29/25/Add.1.
[24] A/HRC/35/9, paras. 23–24.
[25] Pew Research Center, "How social media users have discussed sexual harassment since #MeToo went viral", 11 October 2018.

24. Encryption technologies, pseudonymity and other security features have enabled individuals belonging to minority groups to find one another and create community. The Human Rights Council has stressed that "technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association".[26] The Special Rapporteur asserts that the same is true for the organization and conduct of associations. These tools provide individuals and civil society actors with safe online space to gather and connect with other members of their group as well as to organize and coordinate activities, without undue interference from third parties and government.[27]

25. Through the use of social media, e-petitions and crowdfunding platforms, civil society organizations have been able to reach new audiences, spread information, attract members and find funding in ways that were previously impossible or extremely costly. For example, following the earthquake in Mexico in 2018, a group of citizens mobilized online via #Verificado19S [28] to provide reliable information and assist victims with needed resources. In Turkey, organizations such as Oy ve Ötesi used social media tools to enlist over 60,000 volunteers to monitor more than 130,000 ballot boxes during the general elections of November 2015. In the United States, the American Civil Liberties Union raised millions of dollars in online donations over one weekend in support of its work for immigrants' rights. Similarly, after the Russian Federation had placed severe restrictions on civil society's ability to access foreign resources, the human rights organization OVD-Info used crowdfunding to gather support and raise small, private domestic donations. [29] Similarly, digital technologies have become increasingly important for labour unions to perform their core functions, including organizing protests, keeping in touch with members and providing spaces for discussion and decision-making.[30]

26. Many civil society groups have taken advantage of technology to innovate in addressing social problems. For example, the Landmark project [31] provides publicly available maps and other critical data on lands that are collectively held and used by indigenous peoples and local communities around the world to ensure their protection. The Eyewitness project has developed technologies to enhance the capacity of civil society actors and individuals to document and record human rights abuses.[32] The development of open source software and free commons has been largely driven by civil society organizations such as the Mozilla Foundation and Wikimedia. Platforms such as Signal and Crabgrass have been developed to enhance security of civil society groups' digital communications. Community networks in refugee settlements or in indigenous communities are another example of civil society innovation to address social problems.

27. Digital technologies should be seen by the authorities "as an excellent opportunity to interact with a large and diversified audience prior to and during peaceful assemblies, with a view to sensitizing them on their role and functions, and ultimately building or reinforcing trust among the population".[33] Likewise, States should recognize the value of technology to facilitate people's rights to public participation. The Special Rapporteur welcomes efforts by many governments to establish online platforms through which those interested can submit and collect signatures for petitions on government policies and legislative action.

28. These examples demonstrate a remarkable range of uses of digital technology for the enjoyment of the rights of peaceful assembly and association, and the interplay between offline and online spheres. The Special Rapporteur observes that the rights of freedom of

[26] See Human Rights Council resolution 38/7.

[27] See A/HRC/29/32 and A/HRC/38/35/Add.5.

[28] #Verified19S.

[29] A/HRC/35/28, para. 62.

[30] Jeffrey M. Hirsch, "Worker collective action in the digital age", *West Virginia Law Review*, vol. 117 (2015), pp. 921–959; and Klaus Schoemann, "Digital technology to support the trade union movement", *Open Journal of Social Sciences*, vol. 6, No. 1 (2018), pp. 67–82.

[31] See www.landmarkmap.org.

[32] See www.eyewitnessproject.org.

[33] A/HRC/23/39, para. 74.

peaceful assembly and of association are often seamlessly exercised online and offline. For example, many associations have offices and people meet face-to-face. At the same time, they use digital technology to carry out daily activities and as a space to convene online discussions and assemblies. Similarly, associations primarily based online can also hold in-person discussions and assemblies. The extent of the online and offline activities depends on the association's membership, strategies and goals. Simply stated, international law protects the rights of freedom of peaceful assembly and of association, whether exercised in person, or through the technologies of today, or through technologies that will be invented in the future.[34]

B. Trends in State restrictions

29. The Special Rapporteur is concerned about the variety of measures and tactics that are used by States to control and impede access to and use of digital technology for the exercise of the rights to freedom of assembly and of association. Laws that criminalize online content continue to proliferate, leading to a significant chilling effect on advocacy and mobilization. Numerous jurisdictions have resorted to shutting down access to communications networks and services during elections and public demonstrations, and blocking websites belonging to civil society groups, including human rights organizations. Demonstrating a sophisticated grasp of emerging technical tools, some States – and malicious third-party actors – have increased use of digital surveillance and online harassment against civil society actors, human rights defenders, opposition political leaders and those who plan to stage peaceful public assemblies. All of this has significantly reduced the space in which people can defend and promote shared interests. Notably, the Human Rights Council has expressed concern about "the emerging trend of disinformation and of undue restrictions preventing Internet users from having access to or disseminating information at key political moments, with an impact on the ability to organize and conduct assemblies".[35]

30. This section examines these State actions to determine whether they are compliant with articles 21 and 22 of the Covenant and with the relevant analytical tests set forth in those articles.

1. Legality

31. As already noted, any restrictions on the right to freedom of peaceful assembly and the right to freedom of association must have a legal basis (i.e. be "in conformity with law" or "prescribed by law", respectively),[36] as must the mandate and powers of the restricting authority. The law itself must be sufficiently precise to enable an individual to assess whether or not his or her conduct would be in breach of the law and also to foresee the likely consequences of any such breach.[37]

32. Laws criminalizing access to and use of digital tools are increasingly being adopted, in a diverse range of countries. These laws establish criminal liability in often vague and ill-defined terms, allowing for arbitrary or discretionary application and resulting in legal uncertainty. As such, they fail to meet the legal standards for permissible restrictions under articles 21 and 22 of the Covenant. Examples include cybercrime laws, antiterrorism laws, surveillance laws, and laws against protests.

[34] Douglas Rutzen and Jacob Zenn, "Assembly and association in the digital age", *International Journal of Not-for-Profit Law*, vol. 13, issue 4 (December 2011), p. 67.

[35] See Human Rights Council resolution 38/11.

[36] Article 21 of the Covenant provides that no restrictions may be placed on the exercise of the right of peaceful assembly other than those imposed in conformity with the law. Article 22 (2) provides that "no restrictions may be placed on the exercise of this right other than those which are prescribed by law".

[37] A/HRC/20/27, para. 16; and A/HRC/31/66, para. 30.

Cybercrime laws

33. The prohibition against the use of electronic devices "to ruin communal harmony or create instability or disorder or disturb or is about to disturb the law and order situation",[38] found in the Digital Security Act 2018 of Bangladesh, for example, grants officials excessive discretion to determine what would constitute unlawful conduct and to pursue criminal actions against individuals based on arbitrary and subjective grounds. Authorities could conflate calls for peaceful assemblies on social media with the creation of instability, or ruining communal harmony. Other cybercrime laws give wide-ranging power to governments to block websites deemed critical of the authorities, such as those belonging to human rights defenders,[39] based on broadly defined concepts of national security.

Antiterrorism laws

34. Mandate holders have raised concern on several occasions about the excessively broad language often used in antiterrorism legislation.[40] Although the Special Rapporteur is aware that States have an interest in protecting national security and public safety, which are legitimate grounds for restricting freedom of association and assembly, these laws often are drafted in ways that give opportunities for abuse. For example, many laws include broad and subjective concepts in the definition of terrorism, such as "widespread terror through political extremism", "serious social disturbance",[41] "disrupting public services", "inciting violence at demonstrations" and "creating fear amongst the public to jeopardize the solidarity" of a country.[42] The vagueness of the concepts makes it extremely difficult to determine with reasonable certainty what kind of conduct (online and offline) would be considered "terrorism". Organizations and individuals that are deemed to be promoting or propagating views or beliefs not shared by the majority of the population or that are unfavourable to the authorities are particularly vulnerable. This would lead to a significant chilling effect among them and further exclude them from the digital space.

Surveillance laws

35. Mandate holders have stressed that overly broad and vague surveillance laws often fail to target specific individuals on the basis of a reasonable suspicion.[43] For example, the Investigatory Powers Act 2016, of the United Kingdom of Great Britain and Northern Ireland, contained vague language that allowed authorities to target a group or category of people without requiring each target of the surveillance to be individually identified.[44] Other forms of surveillance law give enormous licence to States to monitor citizens' online activities, such as the Telecommunications and Other Legislation Amendment Bill, of Australia, which includes provisions that would grant authorities unfettered powers to compel companies to facilitate access to encrypted user data for security agencies and weaken encryption technologies.[45] The risks of abuse are increased given that many existing laws and regulations governing surveillance do not keep pace with rapid changes in surveillance technology and its potential uses.

Media and anti-"fake news" laws

36. During consultations with civil society, concerns were raised about the broad language used in Cambodian interministerial decree (*prakas*) No. 170 of 28 May 2018, which prohibits online activities "intended to create turmoil in society". This provision grants authorities excessive discretion to prohibit a wide range of activities online –

[38] See BGD 4/2018, accessible from https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

[39] See, for example, EGY 13/2017.

[40] A/HRC/26/29, para. 59.

[41] See BRA 8/2015.

[42] Asian Forum for Human Rights and Development (Forum-Asia), *Instruments of Repression: A Regional Report on the Status of Freedoms of Expression, Peaceful Assembly, and Association in Asia*, pp. 84 and 89.

[43] See A/HRC/35/28/Add.1.

[44] Ibid.

[45] See AUS 5/2018.

including sharing photos and videos of police abuse against protesters, disseminating messages calling for peaceful demonstrations, and political campaigning. The rules also impose severe penalties, and civil society organizations face the risk of being shut down for disseminating prohibited content, which is disproportionate and incompatible with the right to freedom of association. In addition, these restrictions are imposed through a government decree, adding to legality concerns.[46]

Demonstrations laws

37. In the Russian Federation, for instance, the "Yarovaya Law" introduced overly broad amendments to the Criminal Code that prohibited "inducing, recruiting or otherwise involving" others in the organization of "mass unrest".[47] Publishing statements on the Internet is considered an aggravating factor. Similarly, in Kazakhstan, the Criminal Code forbids providing "assistance" to "illegal" assemblies, including by "means of communication".[48] The broad language of these provisions unduly limits the rights to freedom of peaceful assembly, association and expression, by potentially making it a crime to promote, discuss, seek or link to information regarding a protest event.

2. Legitimate aim

38. Restrictions on the rights to freedom of peaceful assembly and of association must pursue a legitimate aim. The Covenant recognizes only the following aims as legitimate: "national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others". States cannot invoke permissible justifications to conceal illegitimate aims.

Criminalization of online activities

39. Criminalizing the online activities of individuals and organizations constitutes a growing trend in many countries in the world.[49] Individuals are often charged with ill-defined crimes found in antiterrorism, cybercrime and anti-protest laws. Viet Nam, for example, arrested and charged a human rights defender for comments on the Internet allegedly criticizing the Government.[50] The Bolivarian Republic of Venezuela convicted, on crimes of incitement to violence, a political opposition leader calling for anti-government protests on social media.[51] The United Arab Emirates arrested and prosecuted human rights defenders on charges of "circulating false and misleading information on the Internet with a view to spreading hatred and sectarianism"[52] and with using social media to "endanger State security and insult the rulers" under the Cybercrime Law.[53] Egypt arrested and prosecuted activists for "joining an organization founded in violation of the Constitution" and to "undermine State institutions", in retaliation for comments made on social media.[54] In Saudi Arabia, a founding member of the Saudi Civil and Political Rights Association was reportedly sentenced to eight years in prison and an eight-year travel ban for "violating article 6 of the Anti-Cybercrime Law" by "inciting public opinion against the rulers of this country and signing statements that were published online that call on people to demonstrate", and "insisting to not abide by the judicial decision to abolish" the Saudi Civil and Political Rights Association.[55] Saudi women human rights defenders opposing driving bans have been prosecuted in terrorism-related cases, including for "incitement to

[46] Inter-American Commission on Human Rights, "Second report on the situation of human rights defenders in the Americas" (OEA/Ser.L/V/II. Doc. 66), para. 165.
[47] See RUS 7/2016.
[48] A/HRC/29/25/Add.2, para. 57.
[49] A/71/373, paras. 29–35.
[50] See VNM 1/2017.
[51] See Working Group on Arbitrary Detention opinion No. 26/2014.
[52] See ARE 1/2018.
[53] See ARE 5/2013.
[54] See EGY 4/2017.
[55] See SAU 4/2016.

protest", "attempting to inflame public opinion" and "filming protests and publishing on social media".[56]

40. While States often invoke national security and public order concerns when pressing these charges, in reality criminal prosecution is too often used to stifle dissent and control the online space, which is not a legitimate government aim and directly infringes articles 21 and 22 of the Covenant. No person should be held criminally, civilly or administratively liable for organizing, advocating, or participating in a peaceful protest[57] or for establishing or operating an association for a lawful purpose. Dissent is a legitimate part of the exercise of peaceful assembly and association rights and should be protected, online and offline.[58]

Arbitrary blocking of online content

41. Blocking of entire websites of human rights organizations and political opposition parties has become increasingly common in many parts of the world, including in countries of the Middle East and North Africa region. For example, in the United Arab Emirates and in Saudi Arabia, authorities routinely block websites containing online criticism. Websites belonging to civil society organizations and human rights groups are particularly targeted, such as the Saudi #Women2Drive campaign, blocked in 2013. Similarly, Egyptian authorities have blocked several websites of human rights organizations.[59] The firewall employed in China systematically blocks access to thousands of websites and online content based outside China containing key terms such as "democracy" and "human rights".[60]

42. An individual or association's website is an important means for the individual or association to advocate for a cause; to raise issues of public concern and contribute to public debate; to report human rights violations; to publish research; to seek, receive and impart information and ideas of all kinds; to build coalitions and networks with other organizations, including from abroad; to engage in fundraising; to recruit members and volunteers; and to interact with international and regional human rights bodies. In general, the blocking of entire websites is an extreme, disproportionate measure that severely limits the ability to carry out these activities, and therefore undermines the exercise of freedom of assembly and association. In many cases these measures appear to improperly target dissent, and as such, cannot be justified as pursuing a legitimate aim. The Special Rapporteur considers that to prohibit an individual or association from publishing material online "solely on the basis that it may be critical of the government or the political social system espoused by the government"[61] is inconsistent with the rights to freedom of peaceful assembly, association and expression.

Government-sponsored trolling and cyberattacks

43. Some States have harnessed technology to monitor and hamper the work of human rights defenders and civil society actors. Tactics are varied. Many involve hacking phones and computers, issuing death and rape threats, disseminating doctored images, temporarily suspended targets' accounts, hijacking hashtags, spreading conspiracy theories, accusations of treason and promoting virulently discriminatory sentiments. While the Special Rapporteur is mindful that States are not the only perpetrators of these acts, government responsibility for these acts extends into the commissioning and encouragement of such conduct by third parties.

44. These attacks are a direct violation of individuals' rights to freedom of peaceful assembly and of association, as they cannot be justified as pursuing a legitimate aim in a

[56] See SAU 11/2018, and also SAU/1/2017.
[57] A/HRC/31/66, para. 27.
[58] A/HRC/20/27, para. 84.
[59] See EGY 13/2017.
[60] Freedom House, Freedom on the Net 2018, available from https://freedomhouse.org/report/freedom-net/freedom-net-2018. See also Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012), pp. 31–47.
[61] A/66/290, para. 39.

democratic society. Their purpose is the opposite: to intimidate civil society actors, destroy their credibility and legitimacy and deny them the attention necessary for mobilization in the digital space. These attacks undermine the ability of civil society organizations and activists to share or receive information and communicate with others. They create incentives for self-censorship, while threatening individuals' personal security and integrity.

45. For example, trolls are instructed to disseminate propaganda, isolate or drown out critical views, and inhibit anti-government movements, while amplifying the messages of government officials and boosting follower numbers.[62] In Oman, for example, authorities "systematically hack into online accounts and hijack them and flood social media such as Twitter with an endless stream of hashtag references, thus disrupting discussion on specific topics".[63]

46. The use of commercial spyware, such as FinFisher monitoring technology and the Pegasus spyware suite, to launch cyberattacks against civil society actors is another example of this trend. Well-documented reports have linked the Pegasus spyware suite to spyware attacks against activists and human rights defenders in Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia and the United Arab Emirates, among others.[64] These attacks allow hacking into, and watching in real time, their communications, location and activities,[65] and can affect targets both within a State or extraterritorially.[66]

47. Infiltrating social media groups or forums and tracking the online activities of civil society by "friending" activists is another technique used. Open source intelligence can also allow for the pre-emptive disruption of peaceful protests by arresting organizers who are communicating and planning their activities online.

48. Women and lesbian, gay, bisexual, transgender and intersex persons are at particular risk of facing these attacks. For example, the Government of Egypt reportedly identified and arrested lesbian, gay, bisexual, transgender and intersex activists by infiltrating and surveilling their activities on social media platform Grindr.[67] Authorities in Brazil used Tinder to form relationships and then conduct surveillance on women activists engaged in protests.[68] In Thailand, women human rights defenders were subjected to extensive discrediting, harassment campaigns and death threats in blogs and on social media.[69] These attacks take particular forms, which include the dissemination of doctored pictures, usually of a sexualized and gendered nature; the spreading of information designed to discredit, often full of harmful and negative gender stereotypes; violent hate messages and threatening messages on social networks, including calls for gang rape and for murder; and breaches of privacy, including hacking into family members' computers and phones and exposing the phone number, the home address and personal and family photos. The mandate holder echoes the findings of the Special Rapporteur on violence against women, its causes and consequences, that online abuse against women is a direct attack on women's visibility and full participation in public life, and should be duly investigated and punished.[70]

[62] Institute for the Future, "State-sponsored trolling: how governments are deploying disinformation as part of broader digital harassment campaigns" (2018).

[63] A/HRC/29/25/Add.1, para. 34.

[64] See, for example, the Citizen Lab, "Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries".

[65] See LBN 2/2018.

[66] Brief of amici curiae submitted in *John Doe a.k.a. Kidane v. Federal Democratic Republic of Ethiopia* before the United States Court of Appeals for the District of Columbia Circuit.

[67] Article 19, "Apps, arrests and abuse in Egypt, Lebanon and Iran", February 2018.

[68] Privacy International, "State of privacy Brazil".

[69] See, for example, THA 6/2017.

[70] See A/HRC/38/47.

3. Necessary and proportionate to protect a legitimate objective

49. Articles 21 and 22 (2) of the Covenant require that restrictions against the freedom of assembly or of association be necessary and proportionate in a democratic society in the interests of national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others. It has been indicated, under this special procedure mandate, that the word "necessary" means that there must be a pressing social need "for the interference". When such a pressing social need arises, States have then to ensure that any restrictive measures fall within the limit of what is acceptable in a democratic society, which "only exists where pluralism, tolerance and broadmindedness are in place".[71] The onus of establishing this justification always rests on the State.

50. States often impede the exercise of the freedoms of assembly and association online through restrictions that are not necessary or proportionate considering the specific threats invoked. Some examples of this include network disruptions, State-mandated blocking of online content, social media tax, and surveillance using digital technologies.

Network disruptions

51. According to data,[72] at least 40 network disruptions were identified in connection with public demonstrations and peaceful protests in 2018, with 37 in 2017 and 27 in 2016. The regions most affected are Asia and Africa, with cases of Internet shutdowns or social media bans reported in India,[73] the Islamic Republic of Iran,[74] Chad,[75] Cameroon[76] and Togo.[77] India alone accounts for 64 network disruptions related to public demonstrations between 2016 and 2018. Network disruptions amid peaceful assemblies have been reported in other regions of the world, demonstrating that this has become a dangerous global trend. The number of network disruptions and social media bans during elections has also been on the rise since 2016, severely affecting political opposition parties' and social movements' visibility and capacity to mobilize support at a crucial time. These measures affect the capacity of human rights defenders to carry out their work and document human rights abuses.[78]

52. The Special Rapporteur believes network shutdowns are in clear violation of international law and cannot be justified in any circumstances. Shutdowns fail to meet the established test for restrictions on the right to peaceful assembly found in article 21, and for restrictions on the right to freedom of association under article 22 (2), of the Covenant. In most cases, network shutdown orders lack a legal basis. Where a legal basis does exist, shutdown orders are often coupled with broad and vague provisions and lack adequate independent oversight.[79] While these measures are typically justified on grounds of national security and public order, they are a disproportionate – and generally ineffective – means of achieving those legitimate aims.

53. These extreme measures generate a wide variety of harms to human rights, economic activity, public safety and emergency services that outweigh the purported benefits. Network disruptions often backfire and cause chaos and unrest. In the context of protests and elections, when tensions are at their highest, these tools are actually needed to prevent disinformation and dispel rumours, as well as to protect the rights to liberty and personal integrity, by allowing access to emergency help and contact with family and

[71] A/HRC/20/27, para. 17.
[72] Access Now, #KeepitOn campaign, and Shutdown Tracker Optimization Project (STOP).
[73] See IND 5/2016, IND 3/2017 and IND 7/2017.
[74] See IRN 1/2018.
[75] See TCD 3/2016.
[76] See CMR 1/2018.
[77] See TGO 1/2017.
[78] A/68/299, para. 28.
[79] See A/HRC/29/25/Add.2.

friends.[80] The Human Rights Council has unequivocally expressed its concern "at measures in violation of international human rights law that aim to or that intentionally prevent or disrupt access to or dissemination of information online".[81]

Social media tax

54. The Special Rapporteur is concerned that the recent imposition of taxes for the use of social media in some countries may disproportionately affect vulnerable peoples' ability to exercise the freedoms of association and assembly, and that these "social media taxes" may raise concerns of necessity or proportionality. For example, the social media tax in Uganda "disproportionately and negatively impacts the ability of users to gain affordable access to the Internet, and thus unduly restricts their right to freedom of expression and their rights of peaceful assembly and association – particularly so for low-income citizens, for whom purchasing 1 GB of data per month will cost nearly 40 per cent of their average monthly income".[82] While there may be legitimate economic rationales for these taxes, States should take measures to ensure that the taxes do not disproportionately impede the ability of individuals to communicate with other members of society, and widen the digital divides.

Surveillance using digital tools

55. Unnecessary and disproportionate surveillance measures have increased across the world during the past decade. The necessity requirement implies demonstrating how surveillance would achieve a stated purpose, something often jeopardized by the very act of surveillance. States such as Australia and the United Kingdom, for example, assert that national security or public order justifies weakening encryption tools.[83] As stated by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "there is widespread consensus among information security experts that such vulnerabilities impose significant costs on digital security overall, as they may be exploitable by unauthorized third parties even if they are intended solely for government access".[84]

56. The proportionality principle requires proof that the measure used is the least invasive option. Mass surveillance or bulk collection and analysis of all communications metadata[85] – explicitly designed to target associations between individuals – is inherently disproportionate.[86] Similarly, legal requirements on communications service providers to store personal and sensitive data locally and register SIM cards on an indiscriminate basis allow authorities to access information which is not relevant and material to any serious crime or specific threat.[87] Mandatory SIM card registration laws in particular "effectively require the majority of the population to divulge personally identifiable information" to the State concerned.[88] Face recognition technology deployed at large cultural events, major sporting events, music festivals and political gatherings also raises proportionality concerns. Similarly, International Mobile Subscriber Identity capture devices (IMSI catchers)[89] allow countries to collect data from thousands of mobile phones in a specific area, or at public events such as political demonstrations. Such practices are used to identify and surveil all individuals who participate in a particular event or are present in a certain

[80] Jan Rydzak, Global Network Initiative, "Disconnected: a human rights-based approach to network disruptions".
[81] See Human Rights Council resolution 38/7.
[82] See UGA 3/2018.
[83] See A/HRC/35/28/Add.1.
[84] See A/HRC/38/35/Add.5.
[85] Metadata refers to the information associated with a communication, such as geolocation, duration of communication, and who the parties are.
[86] See Human Rights Council resolution 34/7.
[87] A/HRC/29/32, para. 51; and A/HRC/35/22, para. 20.
[88] Ibid.
[89] See A/HRC/35/28/Add.1.

public space.[90] These forms of identification and data collection violate the individual's anonymity in public spaces and exert significant "chilling effects" on decisions to participate in public gatherings.[91]

57. The use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited. Surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision.

C. Digital technology companies: key concerns

58. By virtue of their control of online platforms and tools, these companies are liable to States' requests for access to users' data. At times, such demands may come in the form of informal requests or pressure. Where domestic laws are in violation of international human rights standards and norms, companies are confronted with competing legal obligations that threaten their compliance with human rights as well as their ability to operate in certain jurisdictions. This may result in infringement of users' rights to peaceful assembly and association, and raises questions regarding transparency and accountability. Companies around the world often fail to adequately disclose information about data collection and Governments' requests.[92] Transparency reports issued by major global digital technology companies from the United States and Europe are positive examples that should be scaled up and improved on.

59. The way in which content is moderated by online platforms under their own community standards also raises human rights concerns, including with regard to peaceful assembly and association rights. In particular, the content policies of social media companies reflect varying interpretations of what is acceptable expression and behaviour, which may not be compliant with international human rights standards and norms. Furthermore, the way in which these content policies are enforced through content moderation may also be inconsistent with human rights standards and raise issues of arbitrary interference, despite some attempts at improvements. Enforcement of content policies also seems to affect those with a public profile in a disproportionate manner. In fact, by relying on users to report violations of community standards (i.e. community policing), enforcement of content policies places activists and those calling for mass mobilization at risk of facing arbitrary content removal and account suspension or deactivation. Those with a public profile are not only more likely to be reported than a less popular user (given their visibility) but are also often victims of targeted campaigns aimed at triggering content removal and deactivation. Compounding this problem is the use of artificial intelligence for content moderation, as platforms are increasingly using automated processes to flag content for takedown.

60. Algorithmic systems are also used to influence the findability, visibility and accessibility of the material – meaning what content people see, who they connect with and what groups they find. This means that the delivery of content can be based on historical or inferred political affiliation, or other lines of association, which can be an asset for those trying to reach a particular audience and communicate with like-minded people but is also problematic. Algorithmic systems have the power to silence stories and movements, prevent civil society actors from reaching a wider audience, and reinforce echo chambers or

[90] The Human Rights, Big Data and Technology Project, "The Universal Declaration of Human Rights at 70: putting human rights at the heart of the design, development and deployment of artificial intelligence", 20 December 2018, p. 31.

[91] Daragh Murray and Pete Fussey, "Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data", *Israel Law Review*, vol. 52, issue 1.

[92] Ranking Digital Rights, The Ranking Digital Rights 2018 Corporate Accountability Index, chap. 3, "Inadequate disclosure".

reproduce bias and discrimination, to the detriment of democratic development. These measures can also have a disproportionate effect on already marginalized or at-risk groups, including women.[93] Algorithmic systems are obscure and constantly changing, affecting individuals' and groups' visibility online without them "being able to investigate or understand why, how or on what basis".[94]

61. Policies and features on user privacy and security of communications can also affect the enjoyment of the rights of peaceful assembly and association. Only a few digital technology companies allow the use of pseudonyms or other ways to mask an individual's identity, or provide for encrypted communications. The Special Rapporteur welcomes efforts made by social media platform Grindr to devise and introduce security features on its platform to help protect lesbian, gay, bisexual, transgender and intersex persons in Egypt, the Islamic Republic of Iran and Lebanon who face police harassment, torture and imprisonment.

62. While some efforts to include the right to freedom of expression and the right to privacy in the risk assessments and due diligence processes of some digital technology companies have been taken into account, the Special Rapporteur observes that the rights to freedom of peaceful assembly and of association have not been considered. In his meetings with the digital technology companies, he was able to determine that many such companies recognized the value and importance of these rights in a democratic society, but had not yet issued a high-level policy commitment in that regard.

63. The Special Rapporteur calls on digital technology companies to meet their responsibilities to respect internationally accepted human rights standards, including the rights to freedom of peaceful assembly and of association. To that end, the effective implementation of the Guiding Principles on Business and Human Rights should be a priority for these companies. Models that include an independent impact assessment oversight, such as the ones promoted by the Global Network Initiative,[95] should be scaled up. Digital technology companies should make policy commitments to respect peaceful assembly and association rights (in addition to existing commitments to respect freedom of expression and privacy rights), conduct due diligence in relation to these fundamental freedoms, including through regular human rights impact assessments, and establish effective remediation processes to provide compensation and other forms of redress when violations occur. States should adopt and enforce laws and policies that focus on creating mandatory requirements for digital technology companies to exercise due diligence to identify, prevent, mitigate, and account for how they address, human rights impacts of their business and products, as well as for robust transparency and remediation mechanisms. These laws and policies must "have at their core the objective of universal access and the enjoyment of human rights"[96] and be consistent with guidance following from international standards and norms. They should be adopted only after a fully inclusive and participatory consultation process with the relevant stakeholders.

64. The Special Rapporteur believes the international human rights law framework should govern digital technology companies' responses to government requests, content moderation and engineering choices, including computational curation of content. This means that standards of legality, necessity and legitimacy should be applicable to companies' decisions that affect peaceful assembly and association rights. The Special Rapporteur refers to recent reports of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on the subject of online platforms' content moderation and artificial intelligence, which detail the complexity and extent of these problems and set forth important recommendations.[97]

[93] A/HRC/35/9, para. 41.

[94] A/73/348, para. 32.

[95] Global Network Initiative is a multi-stakeholder platform launched in 2008 "to protect and advance freedom of expression and privacy in the ICT industry by setting a global standard for responsible company decision-making". See https://globalnetworkinitiative.org/team/our-mission/.

[96] Human Rights Council resolution 38/7, para. 18.

[97] A/HRC/38/35, para. 61.

V. Conclusions and recommendations

65. **While the digital age has opened new space for the enjoyment of the rights to freedom of peaceful assembly and of association, it has also brought a range of new threats and risks to these fundamental rights. Severe legal restrictions, and government practices in digital surveillance, for example, risk eliminating the space in which civil society can promote or defend collectively a field of mutual interest. Digital technology companies' actions and inaction have exacerbated these risks or created complex new challenges for individuals and organizations that seek to exercise assembly and association rights online and offline. These challenges are likely to intensify in an increasingly digital future.**

66. **International law protects the rights of freedom of peaceful assembly and of association, whether exercised in person, through technologies of today, or through technologies that will be invented in the future. Existing international human rights norms and principles should not only dictate State conduct, but also be the framework that guides digital technology companies' design, control and governance of digital technologies.**

67. **States should ensure that the rights of peaceful assembly and association are respected, protected and implemented in national legal frameworks, policies and practices, in accordance with international law. Digital technology companies must commit to respect freedoms of peaceful assembly and association and carry out due diligence to ensure that they do not cause, contribute to or become complicit in violation of these rights. In fulfilling their respective responsibilities, States and digital technology companies should comply with well-established principles of non-discrimination, pluralism of views, transparency, multi-stakeholder participation, and access to justice.**

68. **To this end, the Special Rapporteur makes the following recommendations:**

A. Recommendations to States

69. **States should ensure that any interference with the rights to freedom of peaceful assembly and of association is "prescribed by law" and is "necessary in a democratic society in the interests of national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others".**[98] **Restrictions on grounds of "national security", "public safety" and "protection of morals" should be clearly and narrowly defined, so as to prevent their abuse by authorities.**

70. **States should promote and facilitate access to digital technologies, and should not put restrictions on their use for the exercise of the rights to freedom of peaceful assembly and of association. Policies and practices should address equal access to the Internet and digital technologies, the affordability, and participation in the digital age for all, so as to bridge the digital divide.**

71. **Online association and assembly play a particularly important role for marginalized groups, and interference with the rights to freedom of peaceful assembly and of association can have a disproportionate impact on individuals and groups in vulnerable positions. In fulfilling their obligations, States should pay particular attention to the disparate impact that limitations on access to and use of digital technologies can have on racial and religious minorities, political opponents and activists, and lesbian, gay, bisexual, transgender and intersex persons.**

72. **States should ensure that an effective remedy for violation of the rights to freedom of peaceful assembly and of association is available and accessible to all. Remedies should be accessible, affordable, adequate and timely, from the perspective**

[98] Human Rights Council resolution 15/21, para. 4.

of the rights holders affected. States should provide remediation through independent judicial, administrative or legislative authorities or any other competent independent authority provided by the legal system.

73. **States should create an enabling legal framework for the right to peaceful assembly and association in the digital age, by:**

(a) **Repealing, or refraining from introducing, laws that unduly restrict or undermine the rights to freedom of peaceful assembly and of association, including anti-protest laws;**

(b) **Repealing and amending any laws and policies that allow network disruptions and shutdowns, and refraining from adopting such laws and policies;**

(c) **Revising and amending cybercrime, surveillance and antiterrorism laws and bringing them into compliance with international human rights norms and standards governing the right to privacy, the right to freedom of opinion and expression, the right to freedom of peaceful assembly and the right to freedom of association;**

(d) **Promoting and protecting strong encryption and anonymity, including by adopting laws, regulations and policies that confer only on courts the power to remove the right to anonymity, rather than on law enforcement agencies.**

74. **Refrain from, and cease, measures such as cutting off access to the Internet and telecommunications services. Access to Internet and mobile telephony services should be maintained at all times, including during times of civil unrest. Access to and use of digital technologies during elections for assembly and association purposes should be specially respected, protected and promoted.**

75. **End all practices of blocking websites of civil society organizations and human right defenders.**

76. **Prohibit the use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising the right to peaceful assembly and association, both in physical spaces and online.**

77. **Refrain from unduly conducting targeted surveillance using digital tools against civil society actors, protest organizers, minorities and others seeking to exercise their rights to freedom of peaceful assembly and of association. In order to be permissible, targeted surveillance may occur only on the basis that such activities are adopted openly; are time-limited; operate in accordance with established international standards of legal prescription, legitimate aim, necessity and proportionality; and are subjected to continued independent supervision that includes robust mechanisms for prior authorization, operational oversight and review. Individuals and groups should be notified if their rights are breached by surveillance, and effective remedies should be guaranteed.**

78. **Any application of new forms of technological surveillance should also adhere to the above-mentioned principles and standards – including surveillance conducted extraterritorially. States should set up independent inquiries to examine the use of any surveillance technologies, so that the public can assess the manner and frequency of their use, the justifications for and the necessity and proportionality of that use, and whether such technologies are being used in an improper or overly broad way.**

79. **End all acts of government-sponsored online trolling, intimidation and disinformation targeted at civil society actors. States should investigate these acts, provide effective remedies, and adopt and implement preventive measures. In this context, States should identify and address gender-specific forms of online violence and barriers preventing women from accessing justice.**

80. **States should duly implement their duty to protect against abuses of the rights to freedom of peaceful assembly and of association by business enterprises by taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication. This includes adopting and**

enforcing laws and policies that focus on creating mandatory requirements for digital technology companies to exercise due diligence to identify, prevent, mitigate and account for how they address any human rights impacts of their business services and products, as well as for robust transparency and remediation mechanisms. These laws should be adopted only after a fully inclusive and participatory consultation process with all stakeholders.

81. **States should renew their commitments to a multi-stakeholder approach as a cornerstone of Internet governance processes. Effective cooperation on issues relating to the digital sphere depends on the ability of individuals and groups to exercise their rights to freedom of peaceful assembly and of association.**

B. Recommendations to digital technology companies

82. **Companies should meet their responsibility to respect internationally accepted human rights, including the rights to freedom of peaceful assembly and of association, by taking all necessary and lawful measures to ensure that they do not cause, contribute to or become complicit in human rights abuses.**

83. **Companies should adopt a high-level policy commitment to respect freedom of peaceful assembly and association, and recognize the importance of the role of civil society in democracy and sustainable development.**

84. **Companies should seek to prevent or mitigate the adverse human rights impacts of their involvement, to the maximum extent allowed by law, whenever they are requested by States to censor, surveil or monitor individuals or groups or to make available data that they collect, process or retain.**

85. **Companies should recognize international human rights law as the authoritative framework for ensuring that peaceful assembly and association rights are respected in their products and services and should evaluate their policies accordingly. Companies should ensure that their policies and community guidelines are sufficiently clear, accessible and in keeping with international human rights standards. They should also provide more detailed examples or case studies of the way in which their community standards are applied in practice, so that users can understand the circumstances under which personal data or information may be accessed, content may be restricted, or access to the service may be blocked or restricted.**

86. **Companies should exercise human rights due diligence to identify, prevent, mitigate and address violations of the rights to peaceful assembly and association, including by:**

(a) **Undertaking human rights impact assessments which incorporate the rights to freedom of peaceful assembly and of association when developing or modifying their products and services. The process of assessing impacts should always include consultation with civil society actors and other experts and be validated by an accredited external third party with human rights expertise.**

(b) **Integrating the findings of impact assessments, by taking steps to: increase knowledge and awareness of the rights to peaceful assembly and association, by providing training and issuing guidelines to management, employees and other business-linked actors, such as contractors; adopt policies and procedures which set out how the company will assess and respond to government demands for restrictions to communications or access to content; integrate early warning systems within business processes to identify human rights risks, and respond in a timely fashion; use their leverage to challenge government requests that unduly restrict the rights to freedom of peaceful assembly and of association; support the research and development of appropriate technological solutions to online harassment, disinformation and propaganda, including tools to detect and identify State-linked accounts and bots; adopt monitoring indicators that include specific concerns related to freedom of peaceful assembly and association.**

87. **Companies should take effective measures to ensure transparency of their policies and practices, including the application of their terms of service and of computation-based review processes, and respect due process guarantees. To this end, companies should publish regular information on their official websites regarding the legal basis of requests made by governments and other third parties and regarding the number or percentage of requests complied with, and about content or accounts restricted or removed under the company's own policies and community guidelines.**

88. **Companies should introduce independent oversight mechanisms to monitor the outcome of content moderation decisions, and States should consider regulation that requires such independent oversight.**

89. **Companies should establish, in meaningful consultation with the communities affected, operational-level grievance mechanisms that are clearly available and accessible, and are effective in terms of process and remedial outcomes.**

90. **Companies should subscribe to and increase the quality of participation in and implementation of existing multi-stakeholder initiatives. Participating companies should strengthen their role in respecting the rights to freedom of peaceful assembly and of association in the framework of these initiatives.**

91. **Companies should collaborate with governments and civil society to develop technology that promotes and strengthens human rights.**

C. Recommendations to civil society

92. **Civil society actors should continue to innovate and partner with governments, companies and academia to develop technology that facilitates the exercise of the rights to freedom of peaceful assembly and of association.**

93. **Civil society actors should ensure that digital security and digital literacy are at the core of their organization's activities.**

94. **Civil society actors should expand and improve data collection on – and documentation of digital threats to – the rights of association and assembly: in particular with respect to legal developments, network disruptions, surveillance, online harassment and disinformation campaigns. They should share knowledge, promote standards for data collection, and collaborate with other stakeholders in these efforts.**

95. **All civil society groups, not just digital rights organizations, should be supportive and engaged in the process of understanding digital threats to civic space and developing effective responses to threats.**

D. Recommendation to the Human Rights Committee

96. **Consider this report during the elaboration of the general comment on article 21 of the International Covenant on Civil and Political Rights.**