CIVIL SOCIETY
REFERENCE GROUP (CSRG)
In quest for a Conducive and
Enabling Environment for CSOs
in Kenya and the Region

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

CIPESA

KEY ISSUES AND RECOMMENDATIONS

Digital Space and the Protection of Freedoms of Association and Peaceful Assembly in Africa

SUBMITTED TO THE UNITED NATIONS SPECIAL RAPPORTEUR ON THE RIGHT TO PEACEFUL ASSEMBLY AND OF ASSOCIATION - CLÉMENT VOULÉ

INTERCONTINENTAL HOTEL, NAIROBI, KENYA - 21-22 FEBRUARY 2019[1]

A. GENERAL OVERVIEW

Developments in technology have changed the ways society can assemble beyond physical space, the issues that can be discussed, and things that we can do. It has introduced convenience (cost reduction) and promoted inclusivity. However, it has also introduced new dangers and challenges. There is a need to clearly describe what promoting, protecting, respecting and fulfilling rights to freedom of association and assembly (FoAA) entails in the digital era.

Recommendations to States:

1. Consider the adequacy or otherwise of existing laws and international conventions or declarations and strengthen their application in protecting FoAA in the digital era.

2. Commit to domesticate, uphold and fulfill international obligations.

3. Cooperate with international mechanisms for the protection of fundamental freedoms, including voluntary follow-up and reporting on processes like the Universal Periodic Review at the United Nations (UN) Human Rights Council.

[1] Countries represented: Benin, Burundi, Cameroon, Democratic Republic of Congo, Ethiopia, The Gambia, Ghana, Kenya, Malawi, Nigeria, Rwanda, Sierra Leone, South Africa, Tanzania, Togo, Uganda, Zambia and Zimbabwe.

4. Consider expanding or applying laws for the protection of vulnerable groups in the online sphere.

5. Promote research on the impact of digital technologies (both enabling and restrictive) on the exercise of FoAA.

Recommendations to Internet Intermediaries/Telecommunication Companies (Telcos):

1. Commit to respect, protect and fulfill FoAA in accordance with the UN Guidelines on Business and Human Rights.

2. Incorporate FoAA in companies' human rights due diligence framework and practices, including performing human rights impact assessments and providing mechanisms to prevent and mitigate FoAA rights harm through rights-respecting oversight and remedy processes.

B. THE DIGITAL DIVIDE (INCLUDING ITS GENDER, ECONOMIC AND SOCIAL DIMENSIONS)

- Barriers brought by the digital divide are relevant in Africa and include the increasing costs and commercialization of online spaces and infrastructure deficits.

- Access is a primary concern and is deeply gendered issue. In the African context, fewer women and marginalized communities are active in online spaces, and they are specially and disproportionately affected by such barriers.

- Power and agency are also relevant in the online space; there is need to pay attention to unrepresented or under-represented communities, such as rural women and queer people. Such difficulties are exacerbated by class and social divisions; the same inequalities that exist offline also exist online.

- Decentralized internet access and use may reduce cost, increase relevant (African) content, and encourage the formation of community networks that are more likely to meet our specific and contextual needs. However, we remain mindful that localization can create new silos of communication.

Recommendations to States:

1. Guarantee the right to access internet as the foundational right for FoAA in the digital era, and a gendered internet that promotes robust equality and non-discriminatory networks.
2. Promote digital literacy among women and populations at risk.
3. Invest in infrastructure and increase efforts to provide quality access to internet to all, including by facilitating and promoting the establishment of sustainable and autonomous community networks, and points for public access, such as libraries, schools and universities.
4. Guarantee net neutrality in law and practice.
5. Promote adherence to internet freedom standards set at the UN and Regional levels, for example on diversity, access, social justice, privacy and multi-stakeholder governance on the internet.
6. Initiatives to expand internet access should remain open to civil society and community participation.

C. PROLIFERATION OF RESTRICTIVE POLICIES, LAWS AND REGULATIONS

- Governments often draft cybercrime, ICT and other laws in vague and overly-broad terms and selectively apply provisions to persecute activists and control the online and offline activities of the media and CSOs. [Examples: Kenya and Tanzania]
- Recent concerning trends include:
    - mandatory registration of online content creators, including bloggers, online discussion forums, online TV and other social media users [Examples: Egypt (where anyone with more than 5k followers required to register as a media organization), Tanzania and Uganda];
    - imposing prohibitive license fees and onerous responsibilities on online content creators to monitor content and ensure that all content complies with the law;

- taxing "Over The Top" services, broadly defined to include a wide range of social media [Examples: Uganda, Zambia and Benin (although in Benin the tax was reversed following protests]; and
- mandatory SIM card registration [although participants did not reach consensus on whether this is appropriate].

Recommendations to States:

1. Repeal (or revise) laws, regulations and administrative practices that are incompatible with international law protections of FoAA.
2. Promote the adoption of progressive legislation aimed at facilitating FoAA rights online and offline (Example: Nigeria's *Digital Rights and Freedoms Bill*).
3. Maintain dialogue with and amongst all relevant stakeholders in the development of legislation and ensure substantive civil society participation.
4. Train regulators, law enforcement, judicial authorities, legislative bodies and other relevant stakeholders.
5. Promote independent judicial systems that offer good guidance on interpretive issues.

D. NETWORK DISRUPTIONS/INTERNET SHUTDOWNS

- With increasing frequency (and more so since 2016) African governments are disrupting networks and shutting down internet and telecommunication ("telecom") services. Countries recently affected include: Chad, Democratic Republic of the Congo, Gabon, Sudan, and Zimbabwe).
- Shutdowns and/or disruptions have become a particularly disturbing trend in the context of elections and public protests, where governments often impose them under the pretext of preventing the spread of hate speech, disinformation, public disorder and national security.

Recommendations to States, Internet Intermediaries and Telcos:

1. Adopt legal prohibitions of blanket and general interruptions of internet and mobile network communications and services.

2. Strictly adhere to the three-part test of (i) legality, (ii) necessity, and (iii) proportionality to justify any shutdown.

3. Enhance transparency and accountability by government, internet service providers and telecos in the event any network disruption measures are taken.

Recommendations to Civil Society:

1. Promote strategic and public interest litigation to challenge unlawful internet shutdowns and other disruptions [Example: Zimbabwe].
2. Form alliances with telcos and Internet Service Providers to push back against restrictions.
3. Highlight the importance of social media in innovation, business efficiency, and digital and financial inclusion and participation – and the impact of shutdowns on these imperatives.

E. GOVERNMENT SURVEILLANCE AND INSUFFICIENT PRIVACY AND DATA PROTECTIONS

- Targeted surveillance against activists, CSOs and media is growing, and is carried out in complex collaboration between government, the private sector and foreign governments which sell such technology. Violations are exacerbated by the availability and use of new forms of technology, including artificial intelligence (AI), closed-circuit television (CCTV), and facial recognition programs.
- Technology for targeted surveillance advances at a faster rate than legislation.

- There is also increased mass surveillance and data collection by governments and companies through, for example, mandatory sim card registration and data intensive collection of biodata information (for example, by national registries and electoral commissions).

- Security and law enforcement agencies, and telcos and other business entities misuse personal data without adequate judicial and/or parliamentary oversight and accountability [Examples: Chad, Ethiopia, Kenya, Tanzania, Zimbabwe].

- There is lack of transparency in how technology is used, who can access it, and how surveillance and data collection/storage is undertaken. Often there is lack of clarity on which institution has the mandate to surveil/ ask for/ access data from those collecting it. There are inadequate or no data protection laws to address the risks, and little to no independent oversight of these processes.

- The legal framework is inadequate to deal with the proliferation of surveillance technology and data collection, and regulators, lawyers and judiciaries are not equipped to fully understand and protect against the human rights implications.
- These challenges increase the exposure and vulnerability of CSOs, media and activists and has a chilling effect on their use of technology to assert their rights and freedoms.

Recommendations to States:

1. Adopt comprehensive and internationally compliant legal frameworks that provide for all safeguards necessary to protect individuals and groups from surveillance undue interference on their FoAA rights. Laws should provide for clear due process, transparency and oversight safeguards. Civil society should be afforded participation during the design and discussion of policies, laws and regulations.

2. Adopt data protection laws that are consistent with international human rights law and ensure their proper implementation and oversight.

3. Enact laws that protect anonymity and encryption online.

4. Promote surveillance protection legislation that can be more responsive and dynamic to advances in technology.

5. Ensure government and company transparency, including through transparency reports and public reporting to Parliament or independent national commissions.

6. Train law enforcement agents, parliamentarians, prosecutorial and judicial authorities in emerging technology and protection of FoAA in the digital age.

Recommendations to Civil Society:

1. Capacitate the CSO sector, lawyers and other stakeholders to increase their knowledge and understanding of the developing technology.
2. Build specialized competence in data collection and cybersecurity (including through engagement of academics and universities).

F. ONLINE VIOLENCE, INCLUDING VIOLENCE AGAINST WOMEN AND VIOLENCE AGAINST LGBTIQ PEOPLE

- Governments are increasingly using sponsored trolls/bots to discredit and harass activists and political opponents.

- Women are disproportionally affected by this, as well as cyberstalking, online sexual harassment, inappropriate use of private information and promotion/normalization of violence against women. This increases their withdrawal from the public sphere

- For sexual minorities, online space often the last “safe haven” for association, discussion and supportive networks, but the lack of anonymity, the erosion of online privacy, and the negative use of private information has made the online space unsafe.

- Laws offer inadequate protection and law enforcement authorities often ignore or dismiss complaints, due to discrimination or lack of training and capacities.

Recommendations to States:

1. Sanction the use of violence, online harassment and intimidation, and trolling by government and other entities; and negative use of technologies to undermine FoAA and to disrupt communications.

2. Find common definitions for bullying, stalking, doxing, online harassment, threats.
3. Adopt internationally compliant laws that are drafted in precise terms.
4. Train law enforcement agents and judicial authorities to adequately respond and address harassment and online violence complaints.
5. Engage in multi-stakeholder dialogue to find common solutions to online violence and create an enabling environment for civil society's use of the internet.

Recommendations to Civil Society:

1. Promote digital literacy and digital security among internet users, particularly target individuals and groups at most risk, including minority groups.

G. SOCIAL MEDIA CONTENT MODERATION POLICIES AND ALGORITHMS

- Content regulation policies of network platforms, including social media platforms, are vague and are not applied uniformly. Some decisions are automated, others are not, and many decisions are informed by economic interests. Explanations of content take downs vary according to country.
- Algorithms can give visibility to a particular group's message or drown it on the web and so are extremely important for the work of associations and organizers. However, companies' proprietary rights are overly broad and have resulted in too little algorithm information being made publicly available.
- Non-governmental actors are concerned about what data companies share with state actors, as responses to government requests to user's data are inconsistent and their sharing policies lack clarity.

Recommendations to Internet Intermediaries, Telcos and Technology companies:

1. Ensure policies and algorithms are clear, public and do not infringe on FoAA.
2. Adhere to the principle of due process before taking down content.
3. Consider context and culture in decision-making on content take downs.

4. Enhance transparency of policies and algorithms and involve civil society and academia in policy revision processes.

5. Engage in multi-stakeholder dialogue in finding common solutions to online violence and create an enabling environment for the engagement.

Recommendations to Civil Society:

1. Partner with academia and independent experts to promote research on the impact of policies, algorithms and use of online platforms on FoAA.

H. DISINFORMATION

- Disinformation and propaganda campaigns online are commonly used to both target and discredit organizers of gatherings and protests, CSOs and human rights defenders, and increasingly to undermine elections.
- States are enacting anti-disinformation laws as an excuse to target and criminalize content disseminated online by CSOs, while at the same time using the online tools to disseminate disinformation and confuse and silence organizers and activists.

Recommendations to States:

1. Promote digital literacy and digital citizenship that is sensitive and cognizant of existing gender inequalities and/or biases and prevents the spread of disinformation and propaganda online.

2. When drafting legislation to tackle and prevent the spread of disinformation online, ensure it is drafted in clear and precise terms to avoid abuse.

3. Ensure effective and non-discriminatory implementation of the same legislation.

4. Promote further research on the issue of disinformation online.

5. Engage in multi-stakeholder dialogue in finding common solutions to disinformation.

Recommendations to Internet Intermediaries and Telcos:

1. Partner with media companies, civil society and academia to tackle the spread of disinformation online and promote research

2. Develop tech solutions, as well as resources and capacities for civil society to counter and mitigate the spread of disinformation online

For more information, contact:

Civil Society Reference Group: A Kenyan coalition whose role is to protect and enhance an independent and effective civil society voice and agency for public benefit.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA): A leading center for research and analysis of information aimed to enable policy makers in the region to understand ICT policy issues, and for various multi-stakeholders to use ICT to improve livelihoods.

International Center for Not-for-Profit Law (ICNL), an international organisation that has provided technical expertise on enabling legal frameworks for civil society in over 100 countries worldwide and over 20 in Africa.

Participating Organizations[2]

[2] Access Now; Article 19 – East Africa; Article 19 – West Africa; Association for Progressive Communications: All Women Count: Take Back the Tech! (Kenya); Bloggers of Zambia; Centre for Human Rights, University of Pretoria (South Africa); Centre for Human Rights and Rehabilitation (Malawi); Chapter Four Uganda; Civil Society Reference Group (Kenya); Collaboration on International ICT Policy for East and Southern Africa; DefendDefenders (East and Horn of Africa); Dignity Television (Cameroon); Freedom of Expression Hub (Uganda); #GambiaHasDecided (The Gambia); Human Rights Defenders Network – Sierra Leone; International Trade Union Confederation – Africa; Internet Society – Benin Chapter; Inuka Kenya Ni Sisi (Kenya); Jamii Forums (Tanzania); Just City Coalition (Kenya); Kenya Correspondents' Association (Kenya); Legal Aid Service Providers' Network (Uganda); Legal Resources Centre (South Africa); Ligue Burundaise des Droits de l'Homme (Burundi); Ligue des Droites de la Personne dans la Region des Grands Lacs/Observatory of Rights in the Great Lakes Region (Burundi, DRC, Rwanda); Media Institute of Southern Africa – Zimbabwe Chapter (Zimbabwe); Media Policy Research Centre (Kenya); Media Rights Agenda (Nigeria); National Coalition of Human Rights Defenders (Kenya); Nigeria Network of Non-Governmental Organisations (Nigeria); Pan-African Visions (Kenya); Reseau Ouest Africain des Defenseurs des Droits Humains/West African Human Rights Defenders Network (West Africa / Togo); Si Jeunesse Savait (Democratic Republic of Congo); Tanzania Human Rights Defenders Coalition (Tanzania); West Africa Civil Society Institute (West Africa / Ghana).