# Submission: ARTICLE 19 Eastern Africa

2018 IGF Best Practices Forum on Cybersecurity

*We are issuing this Call for Contributions to gain perspectives from all interested stakeholders on existing norms development efforts, how those norms are being implemented and whether they are successful. We're also trying to understand whether differences in design and implementation may result in a "digital security divide": a group of "haves" and "have-nots" in terms of the protection the norms offer.*

## 1. How do you define a culture of cybersecurity?

Here we focus on elements of a culture of cybersecurity that are positive for Freedom of Expression and Right to Information, the core values that guide the work of ARTICLE 19. A rights enabling culture of cybersecurity happens when stakeholders put people, and their rights, at the centre of every policy decision and design. Users and their data, including the data of people who share data in non-digital ways, must be protected by design. This requires human rights to take precedence over corporate interests. Additionally, internet intermediaries and infrastructure providers have a responsibility to ensure cybersecurity that enhances rights. This includes processes and policies that, for example, notify users of instances of data breaches and encourage third-party researchers to responsibly disclose vulnerabilities.

A positive culture of cybersecurity can be fostered by government initiatives that address cybersecurity weaknesses at all levels, including oversight and regulation. Government-led cybersecurity initiatives should not disproportionately transfer burdens on individuals to take responsibility for their own safety and security online.

## 2. What are typical values and norms that are important to you or your constituents?

Keeping the internet on, as demonstrated by the awareness of and participation in the popular campaign #keepiton is a core concern for our constituents. Through the campaign, users have pushed against internet shutdowns and called for secure internet connections especially around elections.

The rights-respecting cybersecurity recommendations, which came out of the Freedom Online Coalition working group "An Internet Free and Secure" have demonstrated value for our constituents and are listed below:

1. Cybersecurity policies and decision-making processes should protect and respect human rights.
2. The development of cybersecurity- related laws, policies, and practices should from their inception be human rights respecting by design.
3. Cybersecurity- related laws, policies and practices should enhance the security of persons online and offline, taking into consideration the disproportionate threats faced by individuals and groups at risk.

4. The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law.

5. Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy.

6. Responses to cyber incidents should not violate human rights.

7. Cybersecurity-related laws, policies and practices should uphold and protect the stability and security of the Internet, and should not undermine the integrity of infrastructure, hardware, software and services.

8. Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy.

9. Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.

10. Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.

11. Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights.

12. Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders

13. Cybersecurity capacity building has an important role in enhancing the security of persons both online and offline; such efforts should promote human rights respecting approaches to cybersecurity.

# 5. Do you have examples of norms that have failed (they have not seen widespread adherence), or have had adverse effects (living up to the norm led to other issues)?

In June 2014, the African Union Convention on Cyber Security and Protection of Personal Data1 text was finalised. AU countries have ratified the Convention, and we encourage all to do so. However, it is worth highlighting here the ways in which the Convention text could have been improved and its potential negative impacts:

- Poor definitions for content restrictions: “child pornography” restrictions were not well defined and overbroad. Conversely, protections for persons against incitement to violence failed to include LGBT.
- “...the Convention fails to put safeguards into the sharing of information between companies and governments2” and does not adequately limit the authority of cybersecurity regulators.

Beyond potential negative impacts, there are aspects of the Convention that are of far more immediate concern:

- The exception to the requirement of user consent in order to process personal data when in “performance of a task carried out in the public interest or in the exercise of official authority” is dangerous.
- Use of a computer to “Insult” someone is banned, yet the term is never defined. In any case, this has the potential to criminalise legitimate speech as defined in international human rights law.
- Technologists and journalists are at increased risk of their work being criminalised due to over broad definitions of “computer fraud” and “fradulently obtained data” in cybercrime provisions.

# 6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?

Policies are implemented, whereas norms are standards that are set with the intention of adoption or influence for policy making. So, taking the question in two parts, we note that:

- The African Union Cybersecurity and Data Protection Convention was an important step to setting norms for African states. The subsequent adoption of the Convention by other African states is working well as some countries have ratified the convention or are slated to do so. And some states have already implemented their own conventions, strategies, policies or legislation. However African states’ adoption of cybersecurity and, in particular, data protection laws is happening at a very slow pace.
- The implementation of cybersecurity and data protection legislations at the national level in Africa is positive in countries where policy decisions, design and implementation considers input and advice from all stakeholders, in particular when civil society is included at each step.

# 7. Within your community, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?

The price of communications can be the biggest driver or deterrent for individuals to adopt best practices with their devices and use of connectivity. However, circling back to our point in response to question #2, the gap between users who are secure when they use digital communications and those who are insecure is not due to the failures or triumphs or individual users. The gap is due to the actors, largely from the private sector, responsible for positive or negative impacts on user data and security, and whether or not the state has taken the initiative to properly regulate those actors.

ARTICLE 19 Eastern Africa recently carried out a study with women journalists. The following research findings support the arguments made above3:

- Most women journalists rely on digital communications for their daily work. This is the breakdown by online services: Facebook (53.7%), WhatsApp (86.4%), e-mail (61.5%) and mobile voice (96.2%).
- Seventy-five percent (75%) of the women journalists interviewed have experienced online harassment in the course of their work.
- Thirty-six percent (36%) of the respondents preferred to ignore the attacks and took no action against the posts or the perpetrators.
- Hacking, stalking and threats appear to be the most common forms of digital harassment of women. Most of the attacks brought to our attention during our research endured for one day.
- Digital harassment leads to women withdrawing from the use of the Internet and in many cases they have stopped working for some time. Our findings indicate that digitally enabled harassment also changed the patterns of online interaction by women.
- When respondents were asked to rate their knowledge of digital security tools and practices, 54% said their knowledge was “good” and 29% said “workable”.
- Most of the digital security tools that women journalists use are built into the devices that use. Their self-reported practises are simple such as using passwords and screen locks.

ARTICLE 19 East Africa regional office