January 29, 2024

Open letter to the Chair of the Ad Hoc Committee on Cybercrime

Your Excellency:

We, the undersigned organizations that work to promote media freedom and freedom of expression across Africa, write to express our deep concern about the potential impact of the proposed Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on freedom of expression and media freedom on the continent. While we recognize the legitimate need to address cybercrime, we strongly believe that this treaty as currently drafted will be abused by authoritarian governments in the region to target and surveil journalists and civil society in contravention of international human rights standards and obligations.

In Africa, national cybercrime laws are already being relied on by some countries to target human rights defenders and journalists and also as a tool to stifle freedom of expression and access to information. These laws often include overbroad and vague content-related crimes, such as criminalizing the publication of false information, hate speech, or the sharing of content online that disrupts public order. Such laws are also characterized by unfettered discretion on state security agents to order Internet shutdowns, snoop on private communications, and weaponize surveillance technologies against the media and human rights defenders. Chilling penalties are prescribed by existing cyber laws failing the prescription of the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (ICCPR) that articulates that the scope of a limitation referred to in the ICCPR shall not be interpreted to jeopardize the essence of the right concerned. Cyber laws applicable in African countries tend to place human rights in peril fundamentally. Freedom of expression, privacy, and access to information are the most flagrantly affected rights.

In Zimbabwe, multiple journalists have been arrested for violating the Cyber and Data Protection Act, 2021. In Niger, a journalist in October 2023 was charged with 'disseminating data likely to disturb the public order,' under the country's 2019 cybercrimes law, which has been used repeatedly against journalists and researchers over the past several years. In Nigeria, multiple journalists have been charged under the country's 2015 cybercrimes law which bans "fake news" and is used to crack down on online expression. In Tunisia, authorities have used the cybercrime decree to detain, charge, or place under investigation at least 20 journalists, lawyers, students, and other critics over their public statements online. In December 2023, two opposition activists were sentenced to imprisonment over speech that is believed to have been genuine expression and criticism of the government.

This adds to the existing pressures that journalists and independent media in Africa are being exposed to, which include physical attacks, surveillance, censorship, restrictions to access information, and damage to equipment and infrastructure, among others.

Extensive research and monitoring by media freedom organizations has revealed the abuse of such laws against journalists in Southern and West Africa. In Nigeria, civil society ended up approaching the ECOWAS Court of Justice for recourse as provisions of the cybercrime law were also being used to 'harass, intimidate, arbitrarily arrest and detain and unfairly prosecute, human rights defenders, activists, journalists, broadcasters and bloggers and social media users who express their views perceived to be critical of the Government both at the Federal and State levels.' The ECOWAS Court declared that Section 24 of Nigeria's cybercrime law which criminalizes sending or causing to be sent an 'offensive, insulting or annoying' message via a computer system is inconsistent and incompatible with Article 9 of the African Charter on Human and Peoples' Rights and Article 19 of the International Covenant on Civil and Political Rights to which Nigeria is a state party.

Across two years of extensive deliberations over a global treaty on cybercrime, civil society, and security experts have expressed grave concerns over the vague and overbroad scope of the treaty text and the lack of strong human rights safeguards. Civil society stakeholders have also made extensive recommendations for improving the treaty text to ensure alignment with existing human rights obligations and frameworks.

We urge the Committee to incorporate the detailed and robust feedback that civil society has shared during the past two years of negotiations. These recommendations will ensure that the treaty is compatible with existing human rights instruments, and has broad-based support from civil society stakeholders in Africa and around the world.

Without consideration of the recommendations made by civil society stakeholders, the repercussions will be dire for human rights in Africa. The overbroad draft treaty provisions would bolster the existing State excesses currently jeopardizing human rights. As drafted, the convention will open the avenue for arbitrary application of national laws, potentially criminalizing legitimate online activities such as journalistic investigations, criticism of government officials, and peaceful dissent. Having an international convention of this kind can also have a chilling effect on online discourse, resulting in a shrinking civic space.

We, therefore, reiterate the following recommendations to the Committee:

- Narrow the scope of the treaty to focus on core cybercrimes like hacking, fraud, and online child exploitation, cyberattacks among others. The treaty should avoid criminalizing legitimate online activities including that content-related crimes should fall outside the scope of this treaty.
- Emphasize clarity and precision by defining key terms and offenses clearly and ensuring consistency with existing international human rights law
- Prioritize robust human rights safeguards including strong provisions that protect freedom of expression, media freedom, and the right to privacy in alignment with existing instruments like the African Charter on Human and People's Rights and the International Covenant on Civil and Political Rights.

- In the international cooperation chapter, an act should be a crime in both countries for international cooperation to be applicable, including the collection and processing of data for investigative purposes. Countries should also be able to decline requests for mutual assistance on grounds that rendering such assistance would threaten fundamental rights and freedoms or risk human rights abuses.
- Ensure that the treaty provides for clear mechanisms, including independent oversight and accountability to safeguard against unlawful and unjustified surveillance.

A global instrument addressing cybercrime must not come at the expense of fundamental human rights. We call upon the Ad Hoc Committee to prioritize the protection of freedom of expression and media freedom in Africa during the ongoing and final negotiations.

We stand ready to work with the Committee to ensure that the final treaty balances the legitimate need to address cybercrime with the critical imperative to protect basic human rights like media freedom and freedom of expression.

Sincerely,

ACTION Namibia Coalition (ACTION)
ADISI-Cameroon
Africa Media and Information Technology Initiative (AfriMITI)
African Academic Network on Internet Policy (AANOIP)
African Center for Youth Development, Education and Advocacy Initiative
African Freedom of Expression Exchange (AFEX)
Article 19 Eastern Africa
Association of Freelance Journalists (AFJ)
Bridges and Hands Foundation
Buytech Global Resources
Centre for Human Rights, University of Pretoria (CHR)
Centre for Human Rights and Rehabilitation (CHRR)
Centre for Journalism Innovation and Development (CJID)
CLEEN Foundation
Collaboration on International ICT Policy for East & Southern Africa (CIPESA)
Committee to Protect Journalists (CPJ)
Cyber Security Experts Association of Nigeria (CSEAN)
DigiCivic Initiative (DI)
Digital Rights Coalition (Malawi)
Digital Rights Lawyers Initiative (DRLI)
Digital Society Initiative
Eastern Africa Editors' Society
Federation of African Journalists (FAJ)
Freedom of Expression Hub (Uganda)
Freedom of Expression Institute (South Africa)

Human Rights Journalists Network Nigeria
International Association of Women in Radio & Television (Kenya -Chapter)
International Press Institute (IPI) Africa Programme
Jonction, Senegal
Kenya ICT Action Network (KICTANet)
Kigali Digital Rights Attorneys
Knowledge House (KHA)
Media Council of Malawi (MCM)
Media Foundation for West Africa (MFWA)
Media Monitoring Africa
Media Rights Agenda (MRA)
Namibia Media Trust (NMT)
Ouestaf News (Senegal)
Paradigm Initiative (PIN)
Reporters Without Borders (RSF)
Rwanda Youth Clubs for Peace organization (RYCLUPO)
Small Media Foundation
Smartclicks Tech-wellness Advocates Network (STAN)
Somali Journalists Syndicate (SJS)
South African National Editors' Forum
The Gambia Information Security Community
Unwanted Witness
Webfala Digital Skills for all Initiative
Zambia Free Press Initiative