Joint Statement Regarding Draft Cybercrime Bill of Sierra Leone

16 April 2021

Access Now and Campaign for Human Rights and Development International (CHRDI) write to the honorable Speaker of the House of Parliament, Dr Abass Bundu, and Minister of Information and Communication, Mr. Mohamed Rahman Swaray, to express our concern over the soon to be passed Sierra Leone draft Cybercrime Bill.[1] While Access Now and CHRDI commend efforts by governments and public authorities geared towards promoting a safe digital space for individuals and to better safeguard their rights, and praise the Minister for welcoming public conversation on the bill[2] and prominently publishing its text, it is clear that laws such as the one in question are far-reaching and could result in human rights abuses. More engagement with civil society, human and digital rights experts, and Parliamentary is needed.

This law does not come into existence in a vacuum. Sierra Leone has in the recent past decriminalized libel and sedition[3], a well-received and applauded move aimed towards promoting free speech and the freedom of expression. In the same breath, authorities have on separate occasions been reported to arrest and prosecute journalists[4] for offences such as insulting members of the armed forces or causing annoyance[5] to people in positions of authority. These, among other occurrences, coupled with the establishment of an independent media commission[6], indicate a worrying trend for the freedoms of expression, press, and

[1] Sierra Leone cybercrime bill, http://mic.gov.sl/Media/News/cyber-crime-act-2020
[2] https://twitter.com/SwarayRahman/status/1374458926855385094
[3] Media Foundation for West Africa, Sierra Leone's parliament repeals criminal libel law that threatens free speech, November 2020.
https://www.mfwa.org/new-dawn-for-sierra-leones-media-as-president-assents-new-law-repealing-criminal-libel/
[4] Media Foundation for West Africa, Sierra Leonean government persecute journalist, activist over social media posts, July 2020
https://ifex.org/sierra-leonean-journalist-relentlessly-persecuted-by-government/
[5] Committee to Protect Journalists (CPJ) Sierra Leone journalist Mahmud Tim Kargbo charged over police reporting, December 2020
https://cpj.org/2020/12/sierra-leone-journalist-mahmud-tim-kargbo-charged-over-police-reporting/
[6] Sierra Leone Legal Information Institute, Independent Media Commission Act 2020

association, and other human rights and fundamental freedoms in Sierra Leone. Sierra Leone, additionally, does not have a data protection law, a necessary foundation and framework for human rights in the digital age.

As the Freedom Online Coalition indicated in its Joint Statement on Human Rights Impact of Cybersecurity Laws, Practices and Policies[7] issued on 7 February 2020 in its meeting in Accra, it is alarming that:

> "*While State authorities are responsible for protecting the human rights of those in their territory and law enforcement should be enabled to assist victims of harmful cyber activities, the FOC is deeply concerned about the practices by some States of asserting excessive control over the Internet under the pretence of ensuring national security while disregarding international human rights law and the principles of an open, free, secure, interoperable and reliable Internet*"

The Freedom Online Coalition's February 2020 statement also provided specific recommendations to States in this area, of which the following are directly relevant to the current discussions in Sierra Leone:

- *States need to comply with their obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation.*
- *States need to develop and implement cybersecurity-related laws, policies and practices in a manner consistent with international human rights law, and seek to minimise potential negative impacts on vulnerable groups and civil society, including human rights defenders and journalists. This includes building, where appropriate, supporting processes and frameworks for transparency, accountability, judicial or other forms of independent and effective oversight, and redress towards building trust. It may also include embedding the principles of legitimacy, legality, necessity or proportionality into policy and practice.*
- *Cybersecurity-related laws, policies, and practices should be developed through ongoing open, inclusive, and transparent approaches that involve all stakeholders.*

The soon-to-be final version of the Sierra Leone National Cybersecurity Strategy speaks to how it "is aimed at facilitating the promotion, protection and enjoyment of fundamental human rights and freedoms of Sierra Leone citizens, as defined in the Sierra Leonean Constitution". Given this, we are concerned that the under-consideration Cybercrime Bill falls short of the

https://sierralii.org/sl/legislation/act/2020/52

[7] https://freedomonlinecoalition.com/news/foc-issues-joint-statement-on-human-rights-impact-of-cybersecurity-laws-practices-and-policies/

government's own strategy, including its position that “all measures taken under this Cybersecurity Strategy will be consistent with Sierra Leone’s international, regional, and national human rights obligations”.

The present cybercrime bill grants sweeping powers to the executive arm of government without establishing a check and balance system that is essential to application of laws in democratic settings and is the very foundation of separation of powers. For instance, section 2 of the act presently states that the President need only consult with the respective minister to institute frameworks that have an effect on the subjects of this law; and even then, the consultation remains optional. In effect, the President can issue legal frameworks on the wide topic of cybercrime without having to seek approval and scrutiny of the legislature. The same section further accords unilateral powers to the President to designate ICT systems as critical infrastructure. Section 48 establishes the National Cyber Security Council that is littered with appointees whose independence may be brought to question since their tenure, both in their qualifying capacity and in their capacity as members of the council, is reliant on the President’s discretion.

The Cybercrime Bill also outlines several legal processes without regard for the rule of law and protections for human rights. Making provisions such as in sections 5 (1) and 7(1) that provide for institution of court proceedings without expressly stating the need and importance of open, adversarial proceedings and specifically the right to be heard, is dangerous territory and serves the possibility of arbitrary application of provisions that fall under those rules. Merely having courts of law determine whether orders should be issued is not enough; unless the matter is of extreme urgency, the rule of law demands that *ex parte* proceedings be expressly limited to extraordinary circumstances. The bill goes on to accord, in section 5(4), powers of discretion to police officers to extend orders to other computer systems without having to seek supplementary orders, a provision open to arbitrary application and abuse.

The cybercrime bill, in addition to this, also establishes imprisonable offences such as in sections 5(7), 7(5), 9(6), 10(6) and Part 5 (on offences) of the act, without defining the specific terms of imprisonment accruing to those offences. The bill leaves it to the Minister concerned to enact subsidiary legislation to address imprisonment terms and, in some cases, fines. It is not acceptable that the framing of punishments for crimes is sub-delegated for the executive branch to define; this has to be done by lawmakers in the main bill itself. Several provisions of the act also encroach on evidentiary law which would be better dealt with in the country’s evidence laws to avoid conflicting application of laws.

The Sierra Leone bill contains a high number of provisions that are far reaching into the territory of data processing; with section 18 of the bill going as far as to establish data sharing

outside the Sierra Leone geographical jurisdiction on the basis of initial preservation requests by other governments seeking search, access, seizure, securing or disclosure of the data. Without a proper data protection legislation or data protection authority, there is no guarantee that the rights of citizens with regard to their data will be protected. To have provisions that go as far as subjecting matters of data processing to presidential orders as found in section 2(2)(g) is an affront to international data protection standards.

Access Now and CHRDI appeal to the members of the Parliament of Sierra Leone to desist from passing the cybercrime bill in its current form. Lawmakers must conduct a deeper review of the bill, with sufficient mechanisms to allow citizens and impacted communities - including human rights defenders and journalists among others - to be able to provide their view, along with soliciting further input from experts. The Sierra Leone Cybercrime Bill must not advance until lawmakers have introduced sufficient amendments that address the glaring human rights issues contained in the draft law. We further appeal to the government of Sierra Leone to accede to and fully implement the Malabo convention.

For more information, contact:

Peter Micek
General Counsel, Access Now
peter@accessnow.org