THE SIERRA LEONE ASSOCIATION OF JOURNALISTS (SLAJ) AND MEDIA REFORM COORDINATING GROUP-SIERRA LEONE (MRCG-SL)

1st Floor, 56 Campbell Street, Freetown / 37 Upper Brook Street, Freetown
Email: slaj.salone@gmail.com/ mrcgonline@gmail.com
Contact: +23276470288 / +23276866519

SIERRA LEONE MEDIA'S POSITION PAPER ON A BILL ENTITLED THE CYBERCRIME ACT, 2020

13th April, 2021

BACKGROUND

On the 29th March 2021, the MRCG and SLAJ held a consultative meeting by bringing together key media stakeholders in Sierra Leone to discuss provisions of the Cybercrime Bill 2020. This follows Parliament's directive to the Ministry of Information and Communications to have further engagements on the cybercrime bill that was being debated. The Bill seeks *"to provide for the prevention of the abusive use of computer systems; to provide for the timely and effective collection of electronic evidence for the purpose of investigation and prosecution of cybercrime; to provide for the protection of Critical National Information Infrastructure; to provide for facilitation of international cooperation in dealing with cybercrime matters and to provide for other related matters."*

The consultative meeting sought the views and opinions of the stakeholders on the Cybercrime Bill 2020 and focused on issues relating to **free speech**, **journalism** and **press freedom** in Sierra Leone.

BACKGROUND

The key media stakeholders included the Independent Radio Network (IRN), Independent Media Commission (IMC), the Right to Access Information Commission (RAIC), Guild of Newspaper Editors (GoE), Sport Writers Association Sierra Leone (SWASAL), Women in the Media Sierra Leone (WIMSAL), Sierra Leone Reporters Union (SLRU), Mass Communication, Fourah Bay College, Sierra Leone Broadcasting Corporation (SLBC), Sierra Leone Court Reporters Association (SLCRA), Parliamentary Press Gallery (PPG), Veteran Journalists Union (VEJU), and Photographers Union. Also in attendance was the Minister of Information and Communications, Mohamed Rahman Swarray and his team.

Following the deliberations and consultations, including presentations from lawyers who argued for and against certain provisions of the bill, the media stakeholders resolved that they were not averse to the enactment of the legislation consistent with international obligations that seek to enhance protection, security and responsible use of cyberspace, but were concerned about the following provisions of the Bill:

CONCERNS

- The title of the bill should be rephrased as **Cybersecurity Bill, 2020** as opposed to Cybercrime Bill, 2020. This is to focus more on the security of the cyber space as opposed to criminalizing it. Ghana for example has a Cybersecurity Act, 2020 which is similar to the draft bill.
- Any section that may criminalize freedom of expression and of the press and the work of journalists and researchers should be **decriminalized** and made civil- including *Section 35*. The bill should include safeguards that protect journalists (especially investigative journalists) with regard their data, identity and confidential sources.

- A Data Protection law should be enacted to accompany the Bill.

- Protection of sources of information should be guaranteed in the Bill.

- A Fact-checking mechanism or team should be setup comprising SLAJ members

- The National Cybersecurity Advisory Council should include SLAJ, RAIC, IMC, civil society members and relevant experts.

CONCERNS

- Clarifications should be made on the Data storage infrastructure and *Section 10* of the Bill which deals with 'interception of content data.'

- The sections in the bill that vested powers in the Minister to make regulation, determine fines and punishment for defaulters should be expunged.

- All terms and expressions in the Bill should be clearly defined and spelled out.

- There should be safeguards to ensure that one cyber investigation does not lead to another unrelated investigation.

- The Bill should be consistent with similar existing laws like the Rights to Access Information Law, Independent Media Commission Act 2020 and the Public Order Amendment Act 2020.

SLAJ and MRCG urge the Ministry of Information and Communication to look into the valid points highlighted in this position paper and act accordingly. SLAJ and MRCG believe that all the points raised, if acted upon, will promote good governance and guarantee freedom of expression.

SPECIFIC PROVISIONS

PART III – POWERS AND PROCEDURES

Section **4** (2)- sounds a bit problematic as it appears evidence can be forcefully taken without following due process.

Section 9 (3)- A period of real-time collection or recording of traffic data under subsection (2) may be extended by a Judge of the High Court for a further specified period of time… **(This extension must also be specified).**

Section 10 (4)- A period of real-time collection or recording of content data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time…. **(This does not indicate period and could potentially be abused with the excuse that investigations are still on-going. Just like the initial application, subsequent ones should indicate coverage period).**

Section 10 (5)- A Judge of the High Court may also require a service provider to keep confidential, an order made under subsection (1) and a warrant issued under subsection (1) of section 5. **(Confidential to even the person being investigated? This could be problematic).**

SPECIFIC PROVISIONS

Section 10 (6)- A service provider who fails to comply with an order under subsection (1) commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe. **(Again giving a minister powers to determine jail terms is problematic as it can arbitrary and unjust).**

Section 21- Subject to this Act, a police officer or other authorised person may, without authorisation:

(a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; **(Without authorization by who? Court? This is problematic and can be arbitrarily misused).**

Or

(b) access or receive through a computer system in Sierra Leone, stored computer data located in a foreign state, if such police officer or other authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system **(This raises data protection and privacy concerns).**

SPECIFIC PROVISIONS

Section 22 (3)- Upon receiving a request under subsection (1), the Attorney- General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute upon the request in accordance with the procedures and powers under this Act or any other law**. (The type of court has to be specified).**

PART V – OFFENCES

Section 25 (1)- A person, including a corporation, partnership, or association, who intentionally and without authorisation causes a computer system to perform a function with intent to secure access to the whole or a part of a computer system or to enable such access to be secured, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

(2) For the purposes of this section, a person secures access to computer data stored in a computer system if by causing a computer system to perform a function he….
(This is very problematic. This means people can be prosecuted for using secure communications such as encryption. The UN resolution on the promotion

and protection of human rights on the internet 2018, urged (particularly in paragraph 9) states to encourage the use of secure digital communications. **"Encourages business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity, and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law;" https://documents-ddsny.un.org/doc/UNDOC/LTD/G18/195/78/PDF/G1819578.pdf?OpenElement**).

(3) For the purposes of this section, "unauthorised" means access of any kind, to a computer system, program or data, by a person who has been authorised to access a specific data in a computer system and without lawful excuse, whether temporary or not, cause a computer system to perform a function other than those authorised, with intent to secure access to the whole or a part of a computer system or to enable such access to be secured. **(Same issue as mentioned above).**

SPECIFIC PROVISIONS

Section 27 (1) (b)- threatens national security; **(If there's no definition of national security this term can be grossly abused so it has to be defined in this Bill to prevent abuse).**

Section 35 (1)- A person, including a corporation, partnership, or association, who individually or with another person, willfully and repeatedly communicates, either directly or indirectly, with another person, if he knows or ought to have known that his conduct **– (This clause is problematic because you can't tell how your messages will be received so if it's said the person 'ought to know,' this will be hard to plead your defence in court).**

35. (2)- A person, including a corporation, partnership, or association, who knowingly or intentionally sends a message or other matter by means of a computer system or network that-

(a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or

SPECIFIC PROVISIONS

(b) he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent... **(This is problematic. There are no clear definitions for these and a plaintiff can allege that they have been annoyed. How is this annoyance determined by a court?). This is subjective and elastic. The word annoyance should be expunged).**

Section 42 (1) (c)- insults publicly through a computer system or network any other person or group of persons distinguished by race, colour, descent or national or ethnic origin, as well as religion; or **(What constitutes an insult under this Act? There needs to be a definition for this else this section is likely to be abused).**

(d) distributes or otherwise makes available, to the public, material which denies or approves or justifies acts constituting genocide or crimes against humanity, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe. **(This part is not clear. "Anyone who denies acts constituting genocide or crimes against humanity." We are not really sure what constitutes the offence with the word 'denies').**

SPECIFIC PROVISIONS

(2) For the purpose of subsection (1), "crime against humanity" includes any of the following acts committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: murders, extermination, enslavement, deportation or forcible transfer of population, imprisonment, torture rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization or any other form of sexual violence of comparable gravity, persecution against an identifiable group on political, racial, national, ethnic, cultural, religious or gender grounds, enforced disappearance of persons, the crime of apartheid, other inhumane acts of similar character intentionally causing great suffering or serious bodily or mental injury; **(It would be good for the section to also include what an insult under this Section also means).**

Section 43 (3)- A person or institution who fails to report an incident of an attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network to the National Computer Security Incidence Response Team within 7 days of its occurrence, commits an offence and is liable to such fine or term of imprisonment as

the Minister may, by Regulation made under this Act, prescribe. **(The word 'intentionally' should be inserted here because depending on capacity, an incident may happen that the said institution or individual may not be aware of it. Again the magnitude and implication of that incident may be lost on the person or the institution such that they won't know if the issue has the potential to influence the functioning of another computer system).**

Section 44. (3)- Notwithstanding subsection (1), where a body corporate is convicted of an offence under this Act, the Court may order that the body corporate shall be wound up and all its assets and properties forfeited to the state. **(This form of remedy is disproportionate- the punishment is too harsh for the offence).**

(4) Nothing contained in this section shall render a person liable to punishment, where he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence. (**Or institution should be added).**

SPECIFIC PROVISIONS

Section 45 (1)- Without prejudice to any contractual agreement between an employer and employee, an employee shall relinquish or surrender all codes and access rights to his employer immediately upon disengagement from employment. **(This may need an expansion to make it clearer).**

Section 48 (1) (m)- Minister of Information and Communications as Secretary**. (A bit odd that the minister will be the secretary to the Council and a Director of Communications under the same ministry will be part of the Council. The minister is above the director of communications of the ministry in terms of hierarchy. The Minister should not be part of the Council and the Council should be politically independent).**

(2) A member of the Council shall cease to hold office if –
(b) the President is satisfied that it is not in the public interest for the person to continue as a member of the Council. **(This is not a reasonable ground especially when public interest is not defined under this Act. This section should be removed).**
Section 51. The Minister may by statutory instrument make Regulations as it considers necessary or expedient for giving effect to this Act. **(This gives the minister too many powers and this can abused).**

SLAJ President

……..

Ahmed Sahid Nasralla

MRCG National Coordinator

……..

Francis Sowa (Ph.D.)