ADVISORY OPINION

30th March 2021

21 SCARY THINGS IN THE CYBERCRIME BILL YOU MIGHT NEED TO KNOW BEFORE IT IS PASSED INTO LAW BY PARLIAMENT

INTRODUCTION

Christian Lawyers Centre hereinafter referred to as LEGAL LINK is a non-profit legal advocacy group comprising of lawyers, law students, philanthropists and human rights activists that seek to defend the rights of religious communities and vulnerable groups in Sierra Leone through legal education, training, advocacy, public interest litigations and the promotion of human rights and respect for the rule of law, accountability, democratic governance and international treaties and conventions to which Sierra Leone is a party.

Since the Cybercrime Bill was laid before Parliament, **LEGAL LINK** has been religiously following the Preliminary Parliamentary debates regarding this proposed bill, the claims, counterclaims and apprehensions from civil rights activists, interest bodies and the wider public as well as the Information Minister's piecemeal response over some of the critical issues that have been raised under the Cybercrime Bill.

While we commend the efforts of the Government of Sierra Leone and in particular, the Minister of Information, for the leadership shown regarding the repeal of the Criminal Libel law **(Part V of the Public Order Act of 1965), LEGAL LINK** is however perturbed and gravely concerned with a plethora of issues enshrined in the proposed cybercrime bill that is currently before the House of Parliament for enactment.

As a leading civil society organization with mandate to advocate for legal and policy reforms in Sierra Leone, our legal team, superintended by the human rights expert and former Commissioner for Human Rights, lawyer Rashid Dumbuya have been able to do a critical examination of the proposed cybercrime bill, bringing out its implications on the human rights and fundamental freedoms of citizens in the state and beyond.

Plausible recommendations for reform of the Bill have also been advanced. This advisory opinion and analysis have been structured into two parts: Part (A) deals with the Concerns; followed by Part (B) Recommendations.

ANALYSIS

Below is a critical analysis of the Proposed CYBERCRIME BILL and its implications on the human rights and fundamental freedoms of citizens in Sierra Leone and abroad.

But before delving into the concerns in the proposed cybercrime Bill, it is vital to first define what a Cybercrime law is.

Cybercrime law identifies standards of acceptable behaviour for information and communication technology users; establishes socio-legal sanctions for cybercrime; protects ICT users, mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online; and facilitates cooperation between countries on Cybercrime matters (UNODC, 2013, p. 52).

Cybercrime law provides rules of conduct and standards of behaviour for the use of the internet, computers and related digital technologies. It prohibits specific types of cybercrime and punishes real-world (offline) crimes (e.g., fraud, forgery, organized crime, money-laundering, and theft) perpetrated in cyberspace and have been made possible with the advent of the internet and internet-enabled digital technologies.

Concern No. 1

The Cybercrime Bill transforms the Minister of Information and Communications into a demi - god and chief judge of the state.

The Minister of Information and Communications is given excessive, enormous and uncontrolled powers under the Cybercrime Bill.

He appears to be a demi-god and chief judge under the said law responsible for not only strategic appointments but also punishing offenders of the Cybercrime law after they would have been convicted by the courts.

By section 25 (1) of the Bill for example, the minister is giving powers to prescribe punishments that should be meted out on convicted persons under the Bill by way of regulations. This is overtly ridiculous to say the least.

Such a provision is tantamount to a coronation of the Minister of Information and Communications as Judge or Chief Justice of the State. **Extending judicial functions to an executive authority is not only dangerous but anathematic to the principles of separation of powers, rule of law and democratic good governance within the state.**

While it is safe to say that best practices across the world do allow for a Minister to formulate regulations that give effect to legislations, the same may not be true for granting the Minister enormous power to prescribe punishments for convicted persons under this bill. This is
certainly an overstretch.

Sentencing of convicted persons is an exclusive reserve work of the judiciary enforced by Magistrates and Judges in accordance with the law or sentencing guidelines. The Minister of Information and Communications is deprived of this legal expertise and acumen.

It is important to also emphasize that the Minister of Information and Communications is a politician and with such powers of punishments at his disposal, he might use it with disaffection to silent opposition politicians, journalists, interest bodies and civil rights activists who may be critical about the excesses of the government to which he is a stakeholder.

Recommendation

The Act must prescribe clear punishments that will be meted out to anyone who contravenes the provisions of the Cybercrime law. The power to determine punishment for offenders of the Cybercrime law must be taken away from the Minister. In a democratic society, it is suicidal to place such powers in the hands

Concern No. 2

Excessive and unlimited powers given to the police or other authorized persons regarding search and seizure of stored computer data

Like the Minister of Information and Communications, the police also enjoy unlimited and excessive powers under this bill. For example, under section 5 of the said bill, the police or other authorized person is given unrestrained powers to institute search and seizure of computer system, program, data and computer data storage materials through an order of a Judge of the High Court for the purposes of serving as evidence in a criminal investigation or proceedings.

Under the proposed Bill, it is irrelevant as to whether the seizure of such data, computer system or storage material breach confidentiality rules or not. Once the police or other authorized person has been able to secure this order from the Court, he will now have the powers to compel any person or entity to produce certain data or information, be it confidential or not.

Without any iota of doubt, this provision of the Bill has the potential to undermine the right to privacy and confidentiality which often characterizes certain professional people like medical doctors, lawyers, and journalists etc compelling them to produce documents that ought to have remained confidential.

Furthermore, by Section 5(4) of the bill, a police officer or other authorized person in the midst of conducting his search warrant or seizure, may even extend his search for data information to a third party whom he reasonably believes has the data in his possession.

The Bill does not require the police officer or other authorized person to resort to the Court again for a separate order to extend search warrant and seizure to third parties.

This is a clear lacuna that will definitely create room for endless human rights violations of the individual privacy rights of citizens. The search warrant and seizure might continue unabated.

Recommendation

The proposed bill must make it mandatory for an order of the court to be sought first before a search warrant and seizure be extended to third parties. Also, exceptions should be given to safeguard confidentiality information, data or agreements being seized at will by police officers.

Concern No. 3

The Bill does not define who an authorized person is

While the proposed Cybercrime Bill gives many powers to an '**authorized person'** in the area of search and seizure, it is interesting to note however that an authorized person is not defined under the interpretation section of the Act.

This omission leaves room for speculations as to who this authorized person will be. Such authorized persons might even include forest guards, marshals, ONS officers, OSD officers and so on and so forth.

Recommendation

Not defining who an **'authorized person'** is under the interpretation section of the bill is a grave omission and must be rectified forthwith so as to avoid abuse of authority by the state.

Concern No. 4

The proposed Cybercrime Bill contains offences with no accompanied penalties and sanctions

Another lacuna that exists under this proposed bill could be seen from the fact that the drafters failed to explicitly prescribe penalties for the many criminal offences that are mentioned under the Act.

It is best practice under legislative drafting for legislations that create offences to equally provide for sanctions and punishments in the event of any breach. This is to ensure that convicted persons are not over-punished or under-punished for the commission of an offence. Sadly to note however, such is not the case in this contested Cybercrime Bill. There is nowhere in the Bill where express penalties are stated for offences committed under the Bill.

This lacuna, in our humble estimation, undermines fair sentencing of an accused person in the criminal justice system and further opens room for arbitrariness and highhandedness in dealing with offenders of this law.

Recommendation

The bill must expressly set out clear- cut sanctions for any offence committed under the Act. Sanctions must not be determined after the commission of the offence. They must be certain and foreseeable.

Concern No. 5

The scope of the Cybercrime Bill extend beyond natural persons

According to the interpretation section of the Act, the word **"person" is defined to include among other things, 'a natural person, a corporation, company, partnership, firm, association or societies'.**

This shows that political parties, civil society organizations, media houses and other interest bodies are not exempted from liability under the Act.

In a democratic society where political parties, civil society organizations and media practitioners play a leading role in holding government accountable, serving as watchdogs and raising awareness on it excesses, this may be quite worrying indeed.

With such provisions, the Cybercrime Bill may be used as a weapon by the ruling government to suppress opposition parties, journalists and civil society organizations that are critical of its policies and programmes.

Recommendation

There is need for the scope of the Bill to be narrowed down to individual persons. Where it is necessary for the Bill to have jurisdiction on corporations, companies, partnerships, firms and associations, clear-cut guidelines must be stated under the Bill to protect political parties, civil society organizations and media houses from being suppressed and invaded illegally.

Concern No. 6

The Bill also sets out to invade into the private rights and activities of Diasporans

Under section 13 and 14 of the proposed Bill for example, the Attorney General and Minister of Justice of the Republic of Sierra Leone is empowered to request from a foreign state assistance that is aimed at investigating or prosecuting offences under this Act; or collecting electronic evidence related to an offence punishable under the laws of Sierra Leone.

By section 14 (2), the Attorney General and Minister of Justice of the Republic of Sierra Leone '**shall communicate directly with the appropriate authority of a foreign state responsible for sending, answering, executing or transmitting requests for mutual assistance or extradition.'**

With such provisions under the Bill, it is certain that the activities of diasporans are no longer immune from invasion by the government of Sierra Leone.

Dissenting voices and groups in the diaspora who may be critical of government's policies and programmes will be of serious target under this bill.

Recommendation

The bill must ensure adequate safeguards for dissenting opinions and critical voices residing in the diaspora to prevent a violation of their civil rights and liberties.

Concern No. 7

The Cybercrime Bill makes room for foreign interference, breach of security, public interest and territorial sovereignty of Sierra Leone

By section 18 of the Bill, **"a foreign state may request or obtain the expeditious preservation of data stored by means of a computer system, located within Sierra Leone, in respect of which it intends to submit a request for mutual assistance, for the search, access, seizure, security or disclosure of the data."**

This foreign request from a foreign state may likely prejudice public and security interests as well as the territorial sovereignty of Sierra Leone.

Recommendation

The Bill must ensure adequate safeguards in order for the public and security interests as well as the sovereignty of the state not to be undermined by rogue regimes abroad over the provision of grants and donor funds giving in exchange for such vital information or persons.

Concern No. 8

The proposed Bill abrogates the rules of evidence in a criminal trial

More negative still, the proposed Cybercrime Bill under section 4 deems all evidence admissible and further shifts the burden of proof to the accused person to showcase why the evidence tendered against him in court is inadmissible.

Section 4 of the said bill read thus: **"In a trial of an offence under any law, the fact that evidence has been generated, transmitted or seized from or identified in a search of a computer system, shall not of itself prevent that evidence from being presented, relied upon or admitted".**

The above section clearly abrogates the rules of evidence in a criminal trial. It is settled law that in a criminal trial, the burden of proof rests with the prosecution. It may only shifts in exceptional circumstances.

Secondly, not all evidence is admissible in a criminal trial. But this seems not to be the case under this law. By section 4 of the Cybercrime Bill, it appears that all evidence (generated, transmitted or seized) will be deemed admissible in the court of law.

Recommendation

The Act must conform to the rules of evidence applicable in criminal proceedings. It is trite law that not all evidence is admissible in a criminal trial.

Concern No. 9

The proposed Bill empowers the police or any authorized person for trans-border access to stored computer data without authorization

Under section 21 of the proposed Bill, the police can access without authorization, publicly available stored computer data, regardless of where the data is located geographically.

Empowering the police or any authorized person to have access to the data of private citizens everywhere in the world and without authorization from them may amount to violation of their privacy rights and civil liberties.

Recommendation

Access to and use of public or private data of citizens by the state must be subjected to due authorization and consent from such citizens. This is quite scary indeed especially for citizens living abroad (diasporans).

Concern No. 10

The composition of the National Cyber Security Advisory Council invites undue political interference into the administration of the Act

The composition of the National Cyber Security Advisory Council as enshrined under section 48 of the proposed bill clearly lays a solid foundation for undue political influence, manipulation and control in the provision of strategic leadership, oversight and guidance on implementation and development of national cyber security legal frameworks in Sierra Leone.

Listed below are the members that comprise the National Cyber Security Advisory Council: The President, the Minister of Finance, the Attorney-General and Minister of Justice, the Minister of Internal Affairs, the Minister of Foreign Affairs and International Cooperation, the National Security Coordinator of ONS, the Director-General of Central Intelligence and Security Unit, the Chief of Defense Staff of the Republic of Sierra Leone Armed Forces, the Inspector-General of Police, the Director-General of National Telecommunications Commission, the Bank Governor, the National Cyber Security Coordinator, the Director of Communications of the Ministry of Information and Communications and the Minister of Information and Communications as Secretary.

It is interesting to note that all of the above Cyber Security Advisory Council members are key political appointees that are largely answerable to, and under the influence and control of the President of the Republic of Sierra Leone. With such kind of makeup, it is obvious that politics would loom large in the oversight, implementation and development of national cyber security legal frameworks in Sierra Leone.

The question remains: why did the composition of the Cyber Security Council not include non-political actors such as members from the Sierra Leone Association of Journalists, civil society organizations, the Sierra Leone Bar Association, Independent Media Commission etc

The reason is simple. The proposed Cybercrime law is another trojan horse and political tool design to suppress political dissent as well as opposing voices both at home and abroad that are critical of the ruling government.

The composition shows that the Cybercrime Bill is an apt replacement of the repealed Criminal Libel Law in fundamental terms.

Recommendation

The composition of the proposed National Cyber Security Advisory Council must be reduced to 7 members and these members must include representatives from civil society, the media, interest groups, women and persons with disabilities.

Inclusion of civil society organizations and interest bodies is critical to striking a balance between upholding fundamental human rights and freedoms of citizens as well as regulating cyber bullying, trafficking in persons and terrorism financing in the cyber space.

Concern No. 11

The grounds upon which a member of the National Cyber Security Advisory Council can be dismissed from office are fluid, weak and nebulous

The proposed Cybercrime Bill under section 47 (2) (b) gives the President arbitrary and unilateral powers to nullify the membership of any member of the National Cyber Security Advisory Council if he is satisfied that it is not in the public interest for the person to continue serving as a member of the Council.

This ground of removal makes for compromise and outright loyalty of Council members to the wishes and desires of the President. It also opens room for political maneuvering and unnecessary dismissals.

The removal process or loss of a member status of a Council member of such an important framework must not be made weak and nebulous. It must be watertight and bulletproofed. Besides, how does the president determines what is not in the public interest?

It is therefore irrelevant as to whether such interception in the transmission of data was done in the public interest or not. Also as far as the Bill is concerned, it is even inconsequential as to whether it was done to expose corruption or not.

Recommendation

The loss of membership in the Advisory Council must be based on clear and reasonable grounds determined by the majority of members and not by one man alone. As a matter of fact, the president's presence in the Council transforms the Council into another cabinet forum. He should therefore be taken out of the composition.

Concern No.12

The quorum that is needed to convene a meeting of the National Cyber Security Advisory Council as well as taking decisions is not known

The proposed CyberCrime bill does not state a specific number of members that can constitute a quorum for the Advisory Council to hold its meeting or take important decisions in a meeting.

It is anyone's guess as to the number of members that may be required to constitute a quorum or to take valid decisions. Why did the drafters omit the number of members that can constitute a quorum for meetings to be held or decisions to be taken? Such silence leaves room for suspicions indeed.

Recommendation

A reasonable number of members that can constitute a quorum for meeting and decision making must be clearly enshrined in the Act.

Concern No.13

Politics looms large in the nomination of the National Cyber Security Coordinator

The proposed Cybercrime Bill under section 47 (1) gives the Minister power to nominate the National Cyber Security Coordinator.

However, no clear guidelines as to how this nomination will be done in a fair and non-partisan manner are stated.

In many cases, when such power is giving to a politically exposed person like the Minister without clear cut guidelines, politics will be the first motivation rather than merit.

Recommendation

Clear cut guidelines as to how the National Cyber Security Coordinator should be recruited must be stated in the Act.

Concern No. 14

The Cybercrime Bill is a Wolfs in sheep's clothing set up to target whatsapp, facebook, twitter and instagram users who express dissenting opinions and criticisms over government policies and programmes

By section 35 (2) of the Cybercrime Bill, '**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 is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another, commits an offence.'**

Many facebook, whatsapp, twitter and instagram users as well as admins of these social medial platforms who share messages that may look indecent or offensive would be under serious target by this law. Civil society activists, journalists and opposition members are also not exempted.

Like the expunged Public Order Act, this section will lead to grave violations of fundamental human rights of citizens by the state. It will also muzzle such rights like freedom of the press, privacy, free speech, the right to assemble and associate and the right to hold opinions in a democratic society.

Recommendation

The Cybercrime Bill must guarantee free speech and free press as enshrined under many international and regional frameworks to which Sierra Leone is a party.

Concern No. 15

Leaks that serve the public interest or exposes corruption are even targeted under the Cybercrime Bill

By section 27 of the Bill, **'a person, including a corporation, partnership, or association, who intentionally and without authorization intercepts or causes to be intercepted non-public transmissions of data to or from a computer system whether directly or indirectly commits an offence.'**

It is irrelevant as to whether such was done in the public interest or not or whether it expose corruption or not. Media houses and practitioners like Africanist Press that engages in leaks so as to help in the exposing of corruption within the state would be seriously targeted under this Bill.

Recommendation

Interceptions and computer leaks that may result in the transmission of data relevant to the public interest as well as the fight against corruption should be made an exception.

Concern No. 16

Cyber/internet cafés would be required to register under NATCOM and the Corporate Affairs Commission

According to section 40 of the CyberCrime Bill, cyber/internet cafes would now be required under the Cybercrime Act to register with NATCOM and the Corporate Affairs Commission.

This change in registration requirement would not only posed an additional burden regarding registration fees but will further provide an opportunity for undue censorship and control of the cyber space as well as internet cafes by NATCOM. It will also make room for easy blockage and unlimited censoring of cyber space by state authorities.

Recommendation

Bringing NATCOM as a registration requirement may be risky as it might open room for abuse and undue censorship of the cyber space and social media. This provision needs to be keenly looked into.

Concern No. 17

The corporate liability provision under the proposed Cybercrime Bill may create opportunity to clamp down on the leadership of opposition political parties

Section 46 (2) of the proposed Bill states thus: **"Where a natural person commits a criminal offence under this Act, for the benefit of a legal person, due to the lack of supervision or control by a natural person, the legal person shall be liable for the offence under this Act."**

This simply means that if a member of a political party for example commits an offence under this Act, the leadership of his political party, for lack of supervision or control, may be held vicariously liable for his offences under this act.

This is ridiculous to say the least and another entrapment to get at the political leadership of political parties that may be critical of the ruling government.

Recommendation

This provision must be amended to reflect individual criminal responsibility for offences committed under the Act. The leadership of political parties must be exempt from liability where they may not be aware of the acts of their supporters given their vast numbers and population size and geographic locations.

It would be overtly impracticable for heads of political parties to supervise and have effective control of their wide spread and diverse supporters at all times.

Concern No.18

Holders of computer passwords in public institutions and MDA's would be under undue pressure and Scrutiny

According to section 31 of the Cybercrime Bill, it states that **"a person, including a corporation, partnership, or association, who intentionally or without authorization discloses to another person a password, access code or other means of gaining access to any program or data held in a computer system commits an offence."**

This provision puts password holders at risk in terms of their jobs. Where any breach occurs in the office even without their knowledge they would be deemed as conspirators.

Recommendation

Safeguards should be provided under this Act for holders of computer passwords within public institutions not to be unduly humiliated and persecuted over leaks that may have nothing to do with them.

Concern No. 19

The Proposed Cybercrime Bill undermines many international human rights laws, treaties and conventions that Sierra Leone has signed and ratified

No doubt, a cursory look at the provisions of the Cybercrime law reveals that it is a law that clearly tramples on the human rights and fundamental freedoms of citizens both within and outside of the country.

This is the case because, the Cybercrime Bill contravenes a good number of international treaties and conventions that Sierra Leone has signed and ratified such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the African Charter on Human and Peoples Rights to name but a few.

Significantly also, even the Malabo and Budapest conventions on cybercrime security have not been spared. The proposed Cybercrime Bill is not in tandem with the spirit, object and purpose of these conventions.

Recommendation

The provisions of the proposed Cybercrime Bill must be tailored to respect human rights and fundamental freedoms and must be in tandem with international human rights laws.

Concern No. 20

The proposed Cybercrime Bill awakens memories of the expunged Criminal Libel Law

The draconian provisions within the Cybercrime Bill, aimed at suppressing dissenting voices, opposition parties, journalists, civil society activists, the mainstream and social media and critics of the political class bring memories of the expunged Public Order Act into the limelight.

As a matter of fact, a leading journalist in Sierra Leone has succinctly described the Cybercrime Bill as the **'NEW PUBLIC ORDER ACT FOR THE ELECTRONIC AGE.'**

The fears expressed by civil society organizations, media practitioners and interest groups regarding the bill have been far and wide reaching.

Little wonder why Parliament has placed a pause on the debating process and called for more sensitization to be done on the Cybercrime Bill by the government.

Recommendation

Provisions that make the Cybercrime Bill resemble that of the expunged Criminal Libel Law should be deleted from the bill and a more robust sensitization and engagement process with civil society organizations, media practitioners and interest groups be ensured to secure a buying-in of the framework by citizens living within and outside of Sierra Leone.

Concern No. 21

The object, spirit and purpose as well as the legitimate expectation of a Cybercrime Bill is overtly misplaced

What is expected of a true Cybercrime law is far removed after one would have read the Sierra Leone version.

Apart from a few plausible provisions like those dealing with child bullying, child pornography etc bulk of the majority of the provisions in the Bill seek to suppress individuals, organizations and entities that make use of electronic devices, social media or cyber space to voice their frustrations, dissenting views and opinions against the ruling government. The Bill largely seeks to regulate the internet and social media.

So many fundamental humans rights would be under serious threat if this Cybercrime Bill is passed into law unamended. Such rights include the right to privacy, hold opinions, assemble and associate, free speech and freedom of the press.

A true and well-meaning Cybercrime legislation should have safeguards that protect citizens human rights and fundamental freedoms.

The legitimate expectation of any Cybercrime Bill is principally to address fraud, money laundering, theft, organized crime, forgery and terrorism related activities which are often carried out in cyber space with intent to undermine national security and public safety.

This is the case for many Cybercrime legislations across the world including the one used in South Africa. But a cursory look at Sierra Leone's Cybercrime Bill would reveal that this legitimate expectation is overtly misplaced.

Rather, the Bill focused more on interfering with the private rights of Citizens both at home and abroad as they interact with the internet, social media and cyber space on a daily basis.

Recommendation

The legitimate expectation of any Cybercrime Bill is to address fraud, money laundering, theft, organized crime, forgery and terrorism related activities that are often carried out in the cyber space with intent to undermine national security and public safety.

The Cybercrime Bill must therefore be amended to have adequate safeguards that will protect citizens' human rights and fundamental freedoms such as the right to privacy, hold opinions, assemble and associate, free speech and freedom of the press.

CONCLUSION

Certainly, this advisory opinion has been done in good faith by LEGAL LINK so as to help ensure a more robust, fairer, human rights- friendly and objective Cybercrime bill that will not undermine and trample upon the fundamental human rights and freedoms of citizens within and outside of Sierra Leone.

It is now up to Parliamentarians and ultimately the President of the country to do the needful.

While we commend the move by the government and in particular, the Minister of Information and Communications to push for the passing of a Cybercrime Act, we appeal that our advisory opinion piece be given due attention as it does not portend, seek or aim to undermine the passing of such a law in the country. Rather, it advocates, promotes and calls for the passing of more measured, human rights - friendly Cybercrime law that addresses legitimate expectations of the people.

It is our candid view that the legitimate expectation of a Cybercrime law should target in fundamental terms money laundering and terrorism financing activities, forgery, theft, organized crime, fraud, trafficking in human beings as well as child pornographic and child bulling that often occurs within the cyber space.

A cybercrime law that sets out to infringe on the enjoyment of human rights and fundamental freedoms of citizens within a democratic society would not only be misplaced but inimical to the national interests and progress of the society. Hence, it should never be entertained.

End

Rashid Dumbuya Esq
Executive Director, LEGAL LINK

On behalf of the Legal Team