Ten dangers of the proposed Cybercrime Law 2020

Augustine Sorie-Sengbe Marrah Esq.
March 23, 2021

1. Section 4(2) of the Cybercrime Bill 2020 states that the fact that evidence has been generated, transmitted or seized from or identified in a search shall not in itself prevent that evidence from being presented, relied upon or admitted. This places a heavy burden on the accused to challenge the authenticity of the digital evidence rather than on the prosecution to prove its authenticity. You might not think much of this until you are a poor journalist or citizen with little or no means or knowledge/expert skills to challenge such digital evidence.
2. Section 5's—search and seizure of stored computer data—power given to the police, pursuant to a search warrant order by a judge, is grossly broad. There is no provision that protects journalists, lawyers, doctors etc. from compelled disclosure of confidential information stored in digital form. By this section, anyone including a journalist might have their right to hold confidential information interfered with or perhaps their means of work and livelihood restricted.
3. Section 5(4) states that where the police believes that the data sought to be seized is stored in another computer, the police officer may extend the search to such other systems. In essence, a police officer may seek for a search warrant from a judge to search or seize the computer of **Ms. A** but by this subsection, he is authorised to extend that search to **Mr. B**, **Sister C** or **Brother D**, **Nephew E, Niece F** and perhaps hundreds of their cousins. There is no provision in this subsection that requires the police to come back to the judge for further authorisation. Although subsection 7 creates an offence for misuse of the search power, we all know what our police are capable of doing. If they can take a photo-frame as evidence, what can't they do given the powers of this law?
4. There is no provision of how and where seized or recorded data or computer system are stored and for how long it can be stored to preserve such information in the event of a discontinuance of criminal investigations. Information critical to journalists and other persons can be severely compromised if there are no such safeguards.
5. Section 7(1) mandates the production of data information by an order of court to the police, from a person or entity based in Sierra Leone or offering their services in SL for e.g. Orange, Facebook, Twitter etc. Under this subsection, all

of one's personal data could be given to the police. Where there is no data protection law providing safeguards, this could be a recipe for disaster especially for social media activism or citizen journalism.

6. Sections 9 and 10 provide for real-time collection of traffic and content data by the police through a service provider by an order of court. These sections also provide that measures shall be taken to maintain the privacy of other users, customers and third parties. But where are the measures? We can't leave them to the conjectures and discretion of the police. Mind you, this order can be given in respect of anyone, members of the opposition, media practitioners, activists etc. Again, where there are no data protection laws, this is dangerous as other critically important data might come into the hands of the police or the service provider during this period and there is no provision for accountability and safeguards.
7. By Section 25, merely using, copying information or downloading data from a website could constitute an offence. Just the copying and transferring to yourself or to a WhatsApp group could be deemed a crime. You don't have to do anything more with the information or data transferred.
8. Section 27 makes it an offence to intercept non-public transmissions of data from a computer system, the transmission of which threatens national security etc. I can easily see Africanist Press and many other investigative journalists falling foul of this a million times over. Because, once you can't state your source, it is deemed unlawfully intercepted. Again, there is no protection for the work of especially investigative journalists in this section.
9. Parent laws create both offences and penalties. The several provisions which give the Minister the power to specify penalties for the various offences is at odds with fair trial rights of accused persons. The laws which create offences should specify the penalties. Statutory legislations do not undergo the same legislative scrutiny as primary legislations. Ministers are granted powers to make rules and procedure but not to determine punishment for offences in a primary legislation. Ministers already have enough powers!
10. Section 35 is the resurrected repealed Part V of the Public Order Act 1965. By subsection 2, sending, sharing defamatory, annoying, insulting, hateful, ill-will etc. messages is an offence. Although, subsection 3 states exclude messages or other matters done in interest of the public, the existence of this provision un-does the gain of the repeal. By the time the courts determine that an activist or a journalist posted something in the interest of the public, they would have spent many days, months and perhaps years on detention, during investigations and

prosecution. As we have always advocated, civil redresses can be legislated, to take care of the Kutubu Koromas and the Adebayors in our society.

Worthy of note is the fact that the words “freedom of expression or right to hold and disseminate information”, a fundamental right is not mentioned in the Act. This law would definitely limit freedom of expression, but no regard has been paid to such fundamental freedom. Similarly, the proposed National Cybersecurity Advisory Council does not have any representative of the Sierra Leone Association of Journalists or the Sierra Leone Bar Association. These two bodies are critical in striking a balance between upholding fundamental right and regulating bad behaviour in the digital space.