CIPESA

Analysis of The South Sudan Cybercrimes and Computer Misuse Provisional Order 2021

November **2021**

Introduction

South Sudan, the youngest country in Africa, requires technological transformation to enable economic development as well as freedom of expression and access to information. Article 22 of the Transitional Constitution of South Sudan 2011 guarantees the right to privacy. South Sudan has also ratified the International Convention on Civil and Political Rights (ICCPR) that provides for the right to privacy under article 17 and the African Charter on Human and Peoples Rights, whose article 5 provides for the right to respect one's dignity, which includes the right to privacy. However, South Sudan is yet to sign and ratify the African Union Convention on Cyber Security and Personal Data Protection.

Information and communication technologies (ICT) are fast evolving in the country, with three mobile operators and 24 licensed internet service providers (ISPs). Indeed, efforts are being placed on the development of the relevant infrastructure,[1] as a result of which technology could spur economic development in the country.[2] Internet penetration is estimated at 16.8%, and 23% of the country's population of 11.29 million is connected to mobile phones.

South Sudan has recently enacted the Cybercrimes and Computer Misuse Provisional Order, 2021 (the Order). While this is timely legislation to counter challenges that come with increased digitalisation, the Order has some concerning provisions for the uptake of ICT and for the enjoyment of online rights and freedoms. This brief explores the pros and cons of the Order.

The Positives

The adoption of the Order reflects South Sudan's commitment to meeting its international duties and obligations envisaged in international and regional human rights standards, especially the ICCPR and the African Charter on Human and Peoples Rights, which call upon states to take all measures necessary to better the human rights of citizens.

The purpose of the Order, under section 3, is to "…protect and prevent any crimes committed through computer or computer system, Internet or any related activities." This reflects the need to protect users of ICT from unscrupulous actors who could potentially defraud others or otherwise commit ICT-enabled crimes and in the long run discourage the use of ICT. The Order is thus timely, given ongoing technological advancement and the digital threats inherent in increased digitalisation.

Majority of the definitions in section 5 are clear and could aid efforts to protect individuals online. However, definitions of "Indecent Content", "Pornography", and "Terrorism" are problematic as explained in the section titled "Overly Broad Definitions".

1 *ITU News, How South Sudan is using ICTs to improve lives, https://news.itu.int/newest-nation-on-earth-using-icts-south-sudan/ .*

2 *Glen Aronson, South Sudan and Technology in 2050, 2019, Better Aid Forum Briefing Paper, https://www.csrf-southsudan.org/wp-content/uploads/2019/09/South-Sudan-and-Technology-in-2050.pdf.*

The jurisdiction of the order in relation to cybercrimes and computer misuse under section 7 provides that cyber criminals could be prosecuted if they are citizens of South Sudan or have committed the crimes against a South Sudanese or if the perpetrators are found in South Sudan. It thus makes strides in recognising the complex nature of prosecuting cybercrimes since they can happen anywhere at any time. The provision labours to cover perpetrators of cybercrimes regardless of where they are physically located, which could enable the prosecution of a wide range of cybercrimes committed against Sudanese nationals and entities.

The Order makes a progressive gesture under section 8 in as far as it provides for the establishment of a specialised unit to investigate and prosecute cybercrimes. Section 8 provides that, "The Minister of Justice may establish a specialised public prosecution attorney unit to investigate and prosecute cybercrime offences under this Provisional Order." If properly and successfully implemented, the provision potentially ensures timely justice since it evisages a unit that could swiftly handle cybercrimes as opposed to the slow justice systems, including courts that are often bogged down by a huge case backlog.

Section 10 on the use of forensic tools to collect evidence is progressive as it provides for the requirement of authorisation by a competent court through an application prior to collecting such evidence. The section provides that: "The use of forensic tools shall be authorised by a competent court through an application, when an investigating authority determines that an essential evidence shall not be collected under this section." In subsection 2, the provision spells out the relevant information to be provided in the application, including (a) the name and address of the suspect, (b) a description of the targeted device or computer system, and (c) a description of the intended measures, purpose, extent and duration of the utilisation of the forensic tools.

Moreover, the information gathered through forensic tools is to be protected against any modification, unauthorised deletion and unauthorised access (subsection 5). Under subsection 6, the authorisation shall be valid for 15 days, and extendable for another 15 days or such other period as court may deem necessary (subsection 7).

The Order, under section 23 (c) and (d), recognises the need to protect children from child pornography and potential sexual exploitation by penalising publication of child pornography and child sex solicitation. Similarly, section 24 prohibits the transmission of child pornography. A person found criminally liable under the section could face up to 10 years of imprisonment, or a fine, or both.

Section 23(c) penalises whoever "publishes child pornography, makes available, facilitates the access of child pornography through a computer or a computer system," while section 23(d) penalises anyone that "proposes, grooms, solicits to meet a child for the purpose of engaging in sexual activities or produces pornographic content using a computer or a computer system."

The Order recognises that the digital space can be used to perpetrate human trafficking and drug trafficking. Section 30 states that, "Whoever establishes, publishes or shares information using a computer or computer system for the purposes of trafficking in human beings or facilitating such a transaction commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding seven years or a fine or both." On the other hand, section 31 provides that, "Whoever creates or publishes or shares information using a computer or computer system for the purposes of trafficking in or distributing drugs or narcotics or facilitating such a transaction commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding ten years or a fine or both." The two provisions, if implemented, could help to combat the complex crimes of trafficking in persons and drugs, which are increasingly perpetrated using online platforms.

The Negatives

Despite the positive elements of the Order as highlighted above, the Order poses a number of threats to digital rights including in the delivery of justice, freedom of expression and access to information, and the right to privacy, as discussed below.

Overly Broad Definitions

While the Order provides a list of definitions that attempt to explain the different terms used, there are challenges related to some of the definitions which could be abused by the state and its agencies. For example, the definition of ***"computer misuse"*** as including among others (a) "what it was not intended to do" and (e) "to alter normal functioning of a computing device, network or any information system asset", is vague and ambiguous. There is no clear scope of what using the computer, devices or information system implies because computers may be designed to perform different tasks while at the same time adapting to changes in technology. Furthermore, it is common knowledge that computing devices could be altered voluntarily or involuntarily during usage. It would be important to specify alteration that could render someone liable under the Order. Similarly, the phrase "alter normal functioning of a computing device, network or any information system" literally includes everything that may not necessarily amount to using a computer to commit a crime. The definition could therefore be used to target government critics in the name of misusing computers.

Further, the definition of ***indecent content*** as "any data, information, audio, image, data message, photo, document, video, graphical representation or symbol that is contrary to the norms and traditions" and the definition of ***pornography*** as "…the representation in books, magazines, photographs, films, and other media, telecommunication apparatus of scenes of sexual behaviour that are erotic or lewd and are designed to arouse sexual interest" present opportunities for abuse of the provision since the phrasing of the two terms is currently presented in a vague manner. The vagueness of the definitions could be used to curtail freedom of expression, media freedom, and access to information. For instance, the government at its discretion could label content to be indecent for being "contrary to the norms and traditions" in order to limit public access to legitimate content and expression online and offline.

The definition of "publish" as "distributing, transmitting, disseminating, circulating, delivering, exhibit, exchanging, barter, printing, copying, selling or offering for sale, letting on hire or offering to let on hire, offering in any other way or making available in any way," has a chilling effect on freedom of expression and access to information.This is because it encompasses all mediums of communicating and sharing of information which may not necessarily amount to publication. The Order needs to concisely define the term publication so as to remove all potential negative impact on freedom of expression and access to information.

Inadequacy of the Oversight Role of Courts

The establishment of a specialised unit by the Minister of Justice under section 8 is a good gesture since it could speed up the justice process for victims. Nevertheless, the powers and functions of the investigating authorities under section 9(1) and 9(2) are too wide and broad. Under the section, investigating authorities are empowered, among others, to access, inspect, seize, collect, preserve data or track data. Moreover, in section 9(3) investigating authorities are empowered to order service providers to hand over data or information related to an information system or device.

The scope of these powers, which lacks judicial oversight such as the requirement to get court orders prior to gaining access to personal data and records, could be misused to the the government's benefit in cases where data of targeted individuals who may be government critics is accessed or received under compulsion by the State or its agencies.

Recommendations

- Expressly provide for a requirement of a court order under section 9(1) and 9(2) as a precursor for access to personal data and records by the state and investigating authorities.
- Delete section 9(3)

Infringement of the Right to Privacy

Section 6 provides for the obligations of service providers. The provision, among others, requires them to store information relating to communications, including personal data and traffic data of communicants, for a period of 180 days. Subsection 6(2) requires service providers and their agents to put in place technical capabilities to enable law enforcement agencies monitor compliance with the Order. While the data storage period of 180 days is much less in comparison to other jurisdictions, and while section 6(1)(d) requires the maintenance of confidentiality, there is no guarantee for personal data protection since South Sudan has no specific law on data protection. Moreover, service providers are required to put in place technical capabilities to enable access to personal data by law enforcement officers.

Recommendations

- Government should swiftly enact a data protection law to guarantee the protection of data of individuals by the various sector players including telecommunication companies and internet service providers.
- South Sudan should ratify the African Union Convention on Cyber Security and Personal Data Protection as an expression of commitment to respecting individual data protection and privacy.
- Service providers should not be compelled to disclose their subscribers' information to law enforcement agencies except on the basis of a court order.

Offences and Penalties

Any law must prescribe sanctions for breach and the sanctions should be actionable and enforceable. However, in prescribing the punishment for the offences including, unauthorised data transmission (section 12), manufacture or possession of unauthorised devices (section 13), disclosure of password or data (section 14), offences committed by means of information systems and technologies (section 15), impersonation (section 16), and offences against the integrity of computer or information systems (section 17), the Order does not specify the fine to be levied on individuals found criminally liable under the Order.

On the other hand, some of the offences provided for under the Order potentially curtail freedom of expression and the right to information. For instance, the offence of spamming under section 21 could be interpreted to include all communications through online platforms including social media platforms like Facebook and WhatsApp. Under the provision, virtually all individuals who forward messages on social media stand the risk of prosecution. This also has a chilling effect on freedom of expression and the right to information.

The offence of offensive communication under section 25 potentially has a chilling effect on freedom of expression, media freedom and access to information. A similar provision under section 25 of the Computer Misuse Act, 2011 for Uganda has been widely used to persecute, prosecute and silence political critics and dissidents.[3] Section 25 of the South Sudan cybercrimes Order could be used in a similar manner to target government critics and dissidents.

3 *See for instance: Stella Nyanzi v Uganda (criminal Appeal No. 0079 of 2019) [2020] UGHCCRD 1 (20 February 2020), https://ulii.org/ug/judgment/hc-criminal-division-uganda/2020/1 ; Ronald Musoke, "Misusing computer misuse law," The Independent, August 5, 2019, https://www.independent.co.ug/misusing-computer-misuse-law/2/ ; CIPESA, Hunting Down Social Media 'Abusers' in Uganda as Elections Near, https://cipesa.org/?wpfb_dl=190*

Recommendations

- Amend the penal provisions to specify fines for violation of each of the respective provisions. In the alternative, the fines should be specified in the rules and regulations.
- The Minister responsible for communication should in accordance with section 35 issue the rules and regulations to prescribe the procedures for implementing the Order.
- Amend the law to restrict unsolicited messages that potentially facilitate disturbance of individuals or that specifically target infringement of individuals' privacy.
- Delete section 25 on offensive communication.

Conclusion

The Provisional Order is timely for South Sudan since it reflects commitment to international human rights obligations. It makes strides in countering cybercrimes which are a major threat to technological advancement, protects children again pornography and sex solicitation, expands jurisdiction for presecution of cybercrimes and fronts the need to counter human and drug trafficking online while at the same providing for judicial oversight over forensic evidence-gathering and potentially quick justice by providing for a specialised unit to investigate and prosecute cybercrimes. However, the Order presents similar measures which have been undertaken in countries like Uganda. It could be used to achieve similar goals which have in recent times been replicated across the region, namely the use of the cybercrime law to target political critics and dissidents as well as the opposition through arrests, arbitrary detention, persecution and prosecution so as to silence them.

CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

+256 414 289 502

programmes@cipesa.org

@cipesaug facebook.com/cipesaug Linkedin/cipesa

www.cipesa.org