CYBERCRIME AND COMPUTER MISUSE BILL, 2024

Arrangement of Chapters and Sections

CHAPTER I

PRELIMINARY PROVISIONS

CHAPTER II

OBLIGATIONS OF SERVICE PROVIDERS AND JURISDICTION OF THE CYBERCRIMES AND COMPUTER MISUSE ACT

CHAPTER III

OFFENCES AND PENALTIES

29. Cyberbullying.
30. Cybersquatting
31. Offenses Relates to Electronic Messages
32. Cyberterrorism.
33. Cyber extortion.
34. Human Trafficking
35. Drug Trafficking
36. Espionage
37. Economic Sabotage
38. Regulations
39. Attempt, conspiracy, aiding and abetting.
40. Spreading of computer virus.
41. Misuse of fake profile.
42. Computer related fraud.
43. Computer-related forgery**.**

CHAPTER IV

ESTABLISHMENT OF THE PROSECUTION UNIT AND PROCEDURAL POWERS OF INVESTIGATION

44. The National Cybercrime Prosecution Unit.
45. Expedited preservation and partial disclosure of traffic data.
46. Production order.
47. Power of access, search and seizure for purposes of investigation.
48. Real-time collection of traffic data.
49. Interception of content data.
50. Deletion order.
51. Limited use of disclosed computer data and information.

CHAPTER V

CRITICAL NATIONAL INFRASTRUCTURE

52. Designation of critical infrastructure.
53. Registration of critical infrastructure.
54. Withdrawal of designation of critical infrastructure
55. Management and compliance audit of critical infrastructure.
56. Duty of owner of critical infrastructure.
57. Access to critical infrastructure.
58. Responsibility of the Authority relating to response to cybersecurity incident.

CHAPTER VI

INTERNATIONAL COOPERATION

CHAPTER VII— GENERAL PROVISIONS

In accordance with the provisions of Article 55(3)(b) read together with Article 85(1) of the Transitional Constitution of the Republic of South Sudan, 2011 (as amended), the National Legislative Assembly, with the assent of the President of the Republic of South Sudan, hereby enacts the following:

A Bill

for

An ACT: to provide for an effective, legal, regulatory and institutional framework to protect the confidentiality, integrity, and availability of computer systems and networks, programmes, and data by preventing unauthorised access, use, or modification; to facilitate the detection, investigation, prevention, prohibition, response, prosecution and punishment of cybercrimes; to ensure the protection of critical national information infrastructure, and promote cybersecurity best practices; for the protection of electronic communications, intellectual property and privacy rights; and for connected purposes.

ENACTED by the Transitional National Legislative Assembly of the Republic of South Sudan:

CHAPTER I

PRELIMINARY PROVISIONS

1. Title and Commencement

This Bill shall be cited to as "the Cybercrimes and Computer Misuse Bill, 2024" and shall come into force on the date of its signature by the President.

2. Repeal and Saving

Any legislation governing the subject of this Bill is hereby repealed; provided that, all actions taken, proceedings, appointments, orders and regulations made or issued thereunder shall remain in force until they are repealed or amended in accordance with the provisions of this Bill.

3. Purpose

The Purpose of this Bill is to—

(1) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes;
(2) ensure the protection of critical national information infrastructure;

(3) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights; and
(4) facilitate international cooperation.

4. Authority and Application

(1) This Bill is drafted in accordance with the provisions of Schedule (A) paragraph (45) of the Transitional Constitution of South Sudan, 2011 (as amended).
(2) The provision of this Bill shall apply to all cybercrimes and computer misuse committed in or outside the Republic of South Sudan.

5. Supersession

Where there is a conflict between the provisions of this Act and the provisions of any other written law, the provisions of this Act shall prevail on matters relating to cybercrime and cybersecurity.

6. Interpretations

In this Bill, unless the context otherwise requires:

"access" means the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network;

"application" means programme or software used to provide electronic or digital services or execution of what the user may need through any means of information;

"Authority" means the National Communication Authority established under section 12 of the National Communication Authority Act, 2012;

"availability" means the ability to make information and related resources accessible as needed, when they are needed, where they are needed**;**

"**communication"** the transmission of information through physical or virtual information communication technology media;

"communication network" means any connection between more than one system or communication;

"communication structure" means private information systems and other sensitive information for provision of service to the public;

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;

"computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes

(a) an information system; and
(b) an operational technology system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system;

"computer data" means any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents or electronic data messages whether stored in local computer systems or online;

"computer program" means a set of instructions executed by the computer to achieve intended results;

"content data" means the communication content of the communication, the meaning or purpose of the communication, or the message or information being conveyed by the communication, other than traffic data;

"confidentiality" means the state of keeping or being kept secret or private.

"critical information infrastructure" means, systems, assets, programme or data that are so vital to the country that their destruction would have an impact on the security, national economic security, national public health and safety of the country;

"critical infrastructure" means a computer or computer system designated under subsection (1) of Section 30;

"cybercrimes" means any crime committed through information system, networks, software, computer, internet or any related activities;

"cybersecurity" means the state in which a computer or computer system is

protected from unauthorised access or attack for the purpose of ensuring that—

(a) the computer or computer system continues to be available and operational;
(b) the integrity of the computer or computer system is maintained; and
(c) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained;

"cybersecurity incident" means any act or attempt, successful or unsuccessful, to gain unauthorised access to, disrupt or misuse an information system or information stored on such information system;

"cybersecurity products" includes

(a) a computer,
(b) a computer system,
(c) a computer programme, or
(d) a computer service designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of another computer or computer system;

"cybersecurity threat" means an unauthorised effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system;

"cyberspace" means the connected network of information technology infrastructure comprising telecom networks, the internet, computer networks, information systems, information processing and control systems and databases where people perform social acts without being limited by space and time;

"data" means numbers, letters, symbols or electronic representations of information in any form stored, processed, generated, produced, transferred to a computer or other electronic device;

"database" means electronic space in which data and information are organised and stored in a way which enable its retrieval or modification;

"device" Includes:

(a) a computer program, code, software or application;
(b) component of computer system such as graphic card, memory card, chip or processor;

(c) computer storage component;
(d) input and output devices;

"digital forensic expert or forensic expert" means an expert with knowledge in the filed of digital forensics by training, practice, experience, certification, formal education on digital forensics or other qualifications;

"Economic sabotage" means actions the use of a computer device or computer system harm the economic interests of the Republic of South Sudan.

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities, and the word "electronically" shall be similarly construed;

"Electronic Communication" means any transfer of a sign, signal or computer data of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, photo optical system in any other similar form physically or virtually;

"Espionage" means the use of computer device or computer system to obtain secret or confidential information on critical infrastructure, security infrastructure and leadership.

"forensics" means the application of investigative and analytical techniques that conform to evidentiary standards, and are used in, or appropriate for, a court of law or other legal context;

"forensic image", also known as a forensic copy, means an exact bit-by-bit copy of a data carrier, including slack, unallocated space and unused space;

"forensic tool" means any investigative tool or device including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks including keystroke logging or collection of investigation information about a use of a computer or computer system by an expert;

"Hosting Provider" means a person who provides service that run servers connected to internet allowing organisation and individual to serve content or host services connected to internet;

"hyperlink" means a symbol, word, phrase, sentence or image that contains path to another source that points to and causes to display another documents when executed;

"indecent content" means any data, information, audio, image, data message, photo, document, video, graphical representation or symbol that is contrary to the norms and traditions;

"information" means includes data, text, images, sounds, codes, computer programs, software and databases;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system;

"integrity" means the accuracy, consistency, and reliability of data;

"interception" means listening to, recording, monitoring or surveillance of the content of communication, including procuring of the content of data, either directly through access and use of computer, a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, when communication is occurring;

"interference" means any impairment to the confidentiality, integrity or availability of a computer system or any program or data on a computer system, or any act in relation to the computer system, which impairs the operation of the computer system, program, or data;

"investigatory authority" means the National Cybercrime Prosecution Unit established by Section 44;

"means of communication" means information and communication devices, including computers, smarts or smart devices or similar related devices;

"Minister" means the Minister responsible for Justice and Constitutional Affairs;

"mobile money" means electronic transfer of funds between mobile phone network subscribers, banks or accounts deposits or withdrawals of funds or payment of bills or processing financial transactions by mobile device;

"national critical information infrastructure" means a vital virtual asset, facility, system, network or process whose incapacity, destruction or modification would have;

(a) a debilitating impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties; or
(b) significant impact on national security, national defence or the functioning of the state.

"network" means a collection of hardware and computers interconnected by communications channels that allow sharing of resources and information;

"**owner of critical information infrastructure**" means the legal owner or operator of the critical information infrastructure and, where the critical information infrastructure is jointly owned by more than one person, includes every joint owner;

"password" means any data by which a computer service or a computer system is capable of being accessed for used;

"pornography" includes 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;

"phishing" means the practice of sending fraudulent communications that appear to come from a legitimate source by email, text message or other forms of communication with the intention to steal money, gaining access to sensitive data and login information, or to install malware on the victim's device;

"public key infrastructure" means a system of hardware, software, policies, and procedures used to create, manage, distribute, and revoke digital certificates that verify the ownership of public keys, allowing for secure online communication and authentication between entities;

"publish" means distributing, transmitting, disseminating, circulating, delivering, exhibit, exchanging, barter, printing, copying, selling or offering in any other way or making available in any way;

"reception" means acquisition of data or information contained in any malicious electronic message;

"service" means use of image, audio, video or data provided over internet or other electronic means;

"Service Provider" means:

(a) a public or private entity that provides to users of its services the means to communicate by use of a computer system; and
(b) any other entity that processes or stores computer data on behalf of that entity or its users;

"Cybersecurity Service Provider" means a person licensed to provide a cybersecurity service;

"spamming" means using messaging systems to send multiple unsolicited messages to a large numbers of recipients for the purpose of commercial advertising, non-commercial proselytising, or any prohibited purpose;

"SS-CIRT" means the South Sudan Computer Incident Response Team established pursuant to section 58;

"subscriber information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established;

(a) the type of communication service used, the technical provisions taken thereto and the period of service;
(b) the subscriber's identity, postal, geographic location, electronic mail address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or
(c) any other information on the site of the installation of telecommunication apparatus, available on the basis of the service agreement or arrangement;

"terrorism" means criminal acts committed by individual or group to further violence or ideological goals streaming from domestic influences political religious, social, racial or environmental nature or associated with, designed foreign terrorist organisation or states sponsor;

"terrorist act" means an act performed in furtherance of a political, ideological, religious, racial or ethnic cause and—

(a) causes serious bodily harm to a person;
(b) causes serious damage to property;

(c) endangers the life of a person;

(d) creates a serious risk to the health or safety of the public;

(e) involves the use of firearms or explosives;

(f) releases into the environment or exposes the public to –

(i) dangerous, hazardous, radioactive or harmful substances;

(ii) toxic chemicals; or

(iii) microbial or other biological agents or toxins;

(g) is prejudicial to national security or public safety;

(h) is designed or intended to disrupt—

i. a computer system or the provision of services directly related to communications;

ii. banking or financial services; or

iii. utilities or transportation;

"traffic data" means any computer data other than the content of the communication, including, but not limited to the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

"unauthorised access" means access of any kind by a person to a programme or data held in a computer without authority if —

(a) the person is not personally entitled to control access of the kind in question to the programme or data; and

(b) the person does not have consent to access the kind of programme or data from the person who is entitled to control access.

"webpage" means any sources of information stored electronically which may be accessed through hyperlinks or any information network; and

"website" means a group of World Wide Web pages usually containing hyperlinks to each other and made available online by an individual, company, educational institution, government or organisation.

CHAPTER II

OBLIGATIONS OF SERVICE PROVIDERS AND JURISDICTION OF CYBERCRIME AND COMPUTER MISUSE ACT

7. Obligations of Service Providers

(1) Without prejudice to the provisions of the National Communications Act, a service provider shall—

(a) keep, store and record information in their system for a continuous period of 180 days including—
    (i) data that enables the identification of the user of the data service related to the information system in which he deals with whenever the service provider is in control;
    (ii) traffic data;
    (iii) data on peripheral devices used in any communication;
    (iv) any other data specified by the National Communication Authority.
(b) take reasonable steps to inform its clients of cybercrimes or other trends which affect or may affect its clients;
(c) disclose abuses to concerned victims and to relevant authorities that infractions have been or are likely to be committed;
(d) maintain confidentiality of the data saved and stored by not disclosing such data without an order from a competent judicial authority, including—
    (i) personal data of any user of their services or any data or information related to the consent and the provided account that users enter into communication with;
    (ii) securing data and information in a way that preserves its integrity and not damaging it;

(2) Without prejudice to the privacy guaranteed under the Constitution, service providers and their agents are obligated to comply with relevant law enforcement agencies in as far as allowing the operation of the law is concerned.

(3) Without prejudice to the provisions of Consumer Protection Act, service providers shall provide their users and specialised government agencies, in the form and method that can be easily accessed directly and continuously, the following data and information:

(a) the name, address, electronic address, information data of the service provider;
(b) any other information that the National Communication Authority considers important for the protection of users.

8. Jurisdiction of Cybercrimes and Computer Misuse

Without prejudice to the provisions of the Penal Code, the provisions of this Act shall apply to any crime committed in or outside the country, which occur in the following cases—

(a) in any means of transportation including vehicle, aircraft or ship registered in the Republic of South Sudan;
(b) by a South Sudanese;
(c) if the victim is a South Sudanese;
(d) if the preparation, planning, direction, supervision and funding as done in the Republic of South Sudan;

(e) if the crime is committed by an organised terrorist group that carries out criminal activities in more than one country including Republic of South Sudan;
(f) by any person, irrespective of his or her nationality, citizenship or location;
(g) if the perpetrator of the crime found in the Republic of South Sudan after its commission and has not been extradited.

CHAPTER III

OFFENCES AND PENALTIES

9. Unauthorized Data Transmission

A person who:
(a) intentionally communicates, discloses or transmits unauthorized computer data, information system, service, program, access code or command to an unauthorized person;
(b) intentionally and unlawfully receives unauthorized computer data or information system;
(c) commits ana offence and upon conviction shall be sentenced to imprisonment for term not exceeding ten years or fine or both.

10. Unlawful possession of devices and computer data.

A person who:
(a) intentionally manufactures, sells, procures for use, imports, distributes or otherwise makes available, a computer system, computer data or any other device, designed or adapted primarily for the purpose of committing any offence under this Bill commits an offence.
(b) intentionally and without authorisation, receives or is in possession of devices and computer data under subsection (1) commits an offence.

A person who commits an offence under this section shall, on conviction, be liable to a term of imprisonment not ***exceeding*** ten years or to a fine not exceeding ***two million pounds*** or***, or to both*.**

In this section —
"possession of any computer data" includes —
(a)having possession of a computer system or device that holds or contains the computer data or computer program;
(b)having possession of a document in which the computer data or computer program is recorded; or
(c)having control of computer data or computer program that is in the possession of another person.

11. Unauthorised access to computer data.

(1) Subject to subsection (2), any person who gains unauthorised access to any program or data held in a computer system commits an offence and is liable on conviction, to a fine not ***exceeding three million pounds*** and a term of imprisonment for a term not ***exceeding three years,*** or to both —

(2) Access by a person to a computer system is unauthorised where the person is not entitled to control access of the kind in question and

(a) is not entitled to control access of the kind in question; and

(b) is not authorised to access of the kind in question by any person who is so entitled.

(3) For the purpose of this section, it is immaterial that the unauthorised access is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

(4) A person is not liable under subsection (1) if that person —

(a) has a right to control the operation or use of the computer system and exercises such right in good faith;
(b) has express or implied consent of the person empowered to authorise him to have such an access;
(c) has reasonable grounds to believe that the person had such consent as specified in paragraph (b);
(d) is acting pursuant to measures that can be taken under this Act; or
(e) is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property.

12. Unauthorised disclosure of password.

A person who, intentionally and without authorisation, discloses any password, access code, biometric authentication, token, two-factor authentication, multi-factor authentication or any other means of gaining access to any computer program or computer data held in any computer system for its production, sale, procurement for use, import or distribution commits an offence and is liable on conviction, to a fine not exceeding ***one million pounds*** and to a term of imprisonment not ***exceeding five years***.

13. Identity theft and impersonation.

A person who fraudulently or dishonestly makes use of an electronic signature, password or any other unique identification feature of any other person commits an offence and is liable, on conviction, to a fine not exceeding one million pounds or to imprisonment for a term not exceeding ten years, or both.

14. Unauthorised interception of computer service

(1) A person who, by any technical means, wilfully intercepts or causes to be intercepted without authorisation, any computer data, or electromagnetic emissions carrying computer data, or non-public transmissions to, from or within, a computer system commits an offence and is liable on conviction to a fine not exceeding ***two million pounds*** or to a term of imprisonment not ***exceeding five years***, or to both.

(2) Where, as a result of the commission of an offence under subsection (1), the operation of the computer system is impaired, or transmitted computer data is suppressed or modified, a person convicted of that offence is liable to a fine not exceeding ***three million pounds*** or to a term of imprisonment not exceeding three ***years***, or to both.

(3) For the purpose of this section, it is immaterial that the unauthorised access or interception is not directed at—
(a) any particular program or data;
(b) a program or data of any kind; or
(c) is acting in the performance of his lawful duties, contractual obligations or is discharging any legal obligation.

15. Unauthorised interference.

(1) A person who, intentionally and without authorisation, hinders the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer commits an offence and is liable on conviction, to a fine not exceeding ***three million pounds*** or to a term of imprisonment for a term not exceeding five ***years***, or to both.

(2) For the purpose of this section, an interference is unauthorised if the person whose act causes the interference—

(a) is not entitled to cause that interference;

(b) does not have consent to interfere from a person who is so entitled.

(3) A person who commits an offence under subsection (1) which;

(a)results in financial loss to any person or organisation;
(b)threatens national security;
(c)causes reputational damage to any person;
(d)causes physical or mental injury to, or the death of, any person;
(e)causes, directly or indirectly, degradation, failure, interruption or obstruction of the operation of a computer system; or
(f)threatens public health or public safety,

is liable on conviction, to a fine not exceeding two million pounds or to a term of imprisonment not exceeding five years, or to both.

(4) For the purpose of this section, it is immaterial whether or not the

unauthorised interference is directed at—

(a) any particular computer system, program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer system.

(5) For the purpose of this section, it is immaterial that an unauthorised interference or any intended effect of it is permanent or temporary.

16. Unauthorised modification of computer data.

(1) Subject to subsection (3), any person who, intentionally and without authorisation, modifies computer data commits an offence and is liable on conviction, to a fine not exceeding ten million pounds or a term of imprisonment for a term not exceeding 10 years, or to both.

(2) Where, as a result of the commission of an offence under this section,

(a) the operation of the computer system;

(b) access to any computer program or computer data held in any computer; or

(c) the operation of any computer program or the reliability of any such computer data,

is suppressed, modified or otherwise impaired, a person who is convicted of the offence shall be liable to a fine not exceeding ***ten million pounds*** or to a term of imprisonment not exceeding ***ten years***.

(3) A modification is unauthorised if—

(a) the person whose act causes it, is not entitled to determine whether the modification should be made; and

(b) the person does not have consent to the modification from any person who is so entitled.

(4) For the purpose of this section, it is immaterial whether an unauthorised modification, or any intended effect of it, is permanent or temporary.

17. Infringement of copyright and related rights.

(1) A person who, without the express authorisation of the author or owner of the copyright—

(a) attempts to use, publish or distribute another person's work for commercial purpose, through a computer system;

(b) downloads movies, music files or pirated software applications for gain or against remuneration; or

(c) posts a copyrighted work such as writing or graphics, online for gain or against remuneration,

commits an offence.

(2) A person convicted under subsection (1) is, on—

(a) a first conviction, liable to a fine not exceeding three hundred thousand pounds or to a term of imprisonment not exceeding two years; and
(b) on a second or subsequent conviction, liable to a fine not exceeding five hundred thousand pounds or to a term of imprisonment not exceeding three years, or to both.

18. Failure to moderate undesirable content.

(1) An administrator of an online account is responsible to moderate and control undesirable content that has been brought to their attention by an investigating authority.
(2) A person who contravenes subsection (1) commits an offence and is liable on conviction, to a fine not exceeding one million pounds and to a term of imprisonment not exceeding five years, or to both.

(3)For the purpose of this section "undesirable content" includes any online content that —
(a)is deceptive or inaccurate, posted with intent to defame, threaten, abuse or mislead the public;
(b)threatens public health or public safety;
(c)threatens national security; or
(d)promotes racism.

19. Wrongful distribution of obscene or intimate images.

A person who transfers, publishes, or disseminates and makes a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person commits an offence and is liable, on conviction to a fine not exceeding one million pounds or imprisonment for a term not exceeding two years, or to both.

20. Publication of False Information

A person who publishes false, deception, fictitious, misleading or inaccurate information or data presented in a picture, text, symbol or another form un a computer system with intent to defame. Threaten, abuse, insult, deceive or mislead the public commits an offense and upon conviction shall be sentenced to imprisonment for a term not exceeding five years or a fine or both.

21. Incitement Through Computer System

A person who incites another person on the basis of race, colour, descent, nationality, ethnic origin or religion or unlawfully publishes or causes to be published through a computer system a material which incites, denies, minimizes or justifies acts constitution an offence. Commits and offence and upon conviction shall be sentenced to imprisonment for a term not exceeding ten years or a fine of both.

22. Spamming.

A person who engages in spamming with intent to disrupt the operations of a computer be it public or private or financial institutions commits an offence and is liable on conviction to a term of imprisonment not exceeding five years or a fine not exceeding one million pounds, or both.

23. Phishing.

A person who knowingly or intentionally engages in computer phishing or with intent to commit an offence –

(a) initiates the transmission of unsolicited messages;

(b) relays or retransmit unsolicited messages; or

(c) falsifies header information in unsolicited messages;

is liable on conviction to fine not exceeding one million pounds or to imprisonment for a term not exceeding five years, or to both.

24. Pornography.

A person who publishes of causes to published through a computer system or through any other information and communication technology pornography, or pornography which is lascivious or obscene; commits an offence and is liable on conviction, in the case of publication of—

(a) pornography, to a fine of not less than five million pounds or to imprisonment for a term not exceeding fifteen years or to both;

(b) pornography which is lascivious or obscene, to a fine of not exceeding five million pounds or to a term of imprisonment not exceeding fifteen years or to both.

25. Revenge Pornography.

A person who, by means of a computer system, discloses or publishes a sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress, commits an offence and is liable on conviction, to a fine not exceeding *two million pounds* or to a term of imprisonment not ***exceeding ten years, or to both.***

26. Child pornography and related offences.

(1) A person who intentionally uses any computer system or network in or for —

(a) producing child pornography;

(b) distributing or transmitting child pornography;

(c) procuring child pornography for oneself or for another person;

(d) possessing child pornography in a computer system or on a computer-data storage medium:

commits an offence under this Bill and is liable on conviction –

(i) in the case of paragraphs (a), (b) and (c) to imprisonment for a term of 15 years or a fine of not more than two million pounds or to both fine and imprisonment; and;

(ii) in the case of paragraphs(d) of this subsection, to imprisonment for a term not exceeding ten years or a fine of not exceeding two million pounds or to both.

(2) A person who, intentionally proposes, grooms or solicits, through any computer system or network, to meet a child for the purpose of:

(a) engaging in sexual activities with the child;

(b) engaging in sexual activities with the child where –

(i) use is made of coercion, inducement, force or threats;

(ii) abuse is made of a recognized position of trust, authority or influence over the child, including within the family; or

(iii) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence;

(c) recruiting, inducing, coercing, exposing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes;

commits an offence under this Bill and is liable on conviction—

(i) in the case of paragraphs (a) to imprisonment for a term not 15 years and a fine of not more than one million pounds; and

(ii) in the case of paragraphs(b) and(c) of this subsection, to a fine not exceeding three million pounds or to a term of imprisonment not exceeding fifteen years or to both.

(3) For the purpose of subsection (1), the term “child pornography” includes pornographic material that visually depicts—

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; and

(c) realistic images representing a minor engaged in sexually explicit conduct.

27. Offensive Communication

A person who intentionally uses electronic device to pass communication that is deemed harmful, abusive, or inappropriate, potentially causing harm or distress to others commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding two years or a fine or both.

28. Cyberstalking

A person who intentionally and repeatedly uses electronic communication to track or monitor with intent to harass or cause fear to another person commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding four years or a fine or both.

29. Cyberbullying.

A person who, individually or with other persons, commits cyberbullying, commits an offence and is liable on conviction, to a fine not exceeding ***two million pounds*** to a term of imprisonment not exceeding ***ten years, or to both***.

30. Cybersquatting

A person who intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network without consent commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding three years or a fine or both.

31. Offenses Relates to Electronic Messages

A person who:

(a) unlawfully induces any person in charge of electronic devices to deliver any electronic messages not specifically meant for him or her;
(b) unlawfully hides or detains any electronic mail, message, electronic payment, credit and debit card which was found by the person or delivered to the person in error and which ought to be delivered to another person;
(c) unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed;
(d) transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person;
(e) knowingly and without authority causes any loss of property to another by altering erasing, inputting or suppressing any data stored in a computer
(f) sends an electronic message which materially misrepresents any fact upon which reliance by another person is caused to suffer any damage or loss;
(g) with intent to defraud, franks electronic messages, instructions, subscribes any electronic messages or instructions; or
(h) manipulates a computer or other electronic payment device with the intent to short pay or overpay.

Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding three years or a fine or both.

32. Cyberterrorism.

A person who intentionally accesses or causes to be accessed a computer system or network for the purpose of carrying out an act of terrorism, commits an offence is liable on conviction, to a fine not exceeding ***Two million pounds*** or to a term of imprisonment not ***exceeding ten*** years.

33. Cyber extortion.
A person who engages in cyber extortion commits an offence and is liable on conviction, to a fine not exceeding ***one million pound*** or to a term of imprisonment ***not exceeding ten years***.

34. Human Trafficking

A person who 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.

35. Drug Trafficking

A person who creates, publishes or shares information using a computer or computer system for the purposes of trafficking in or distributing drugs or narcotics or facilitating such transaction commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding ten years or a fine or both.

36. Espionage

A person who uses a computer or computer system to conduct espionage activities. Commits an offence an offence as provided for in the National Security Act.

37. Economic Sabotage

A person who uses a computer or a computer system to engage in activities related to economic sabotage including, but not limited to, tax evasion, interference with revenue collection or its disbursement and money laundering commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding three years or a fine or both.

38. Regulations

The Minister may issue rules and regulations for effective and efficient implementation of this Bill.

39. Attempt, conspiracy, aiding and abetting.

A person who —
(a) attempts to commit any offence under this Act; or

(b) aids, abets, conspires, counsels or procures another person(s) to commit any offence under this Act:

commits an offence and is liable on conviction to the punishment provided for the principal offence under this Act.

(c) An employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using computer system(s) or network, commits an offence and is liable on conviction to imprisonment for a term of not more than seven years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.

40. Spreading of computer virus.

A person who engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers commits an offence is liable on conviction to a term of imprisonment of 3 or a fine not exceeding one million, or to both.

41. Misuse of fake profile.

A person who individually, or with other persons, makes use of a fake profile to cause harm commits an offence and is liable on conviction, to a fine not exceeding ***one million pound or to a term of imprisonment not exceeding five years.***

42. Computer related fraud.

A person who, intentionally and without authorisation, causes loss of property to another person by—

(a) any input, alteration, deletion, delaying transmission or suppression of computer data; or;

(b) any interference with the functioning of a computer system,

to procure on their behalf or on behalf of another person, any form of advantage commits an offence, and is liable on conviction, to a fine not exceeding **two million pounds** or three times the value of undue advantage received, whichever is greater, or to a term of imprisonment not **exceeding ten years**.

43. Computer-related forgery.

(1) A person who, intentionally and without authorisation, inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data, with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible, commits an offence and is liable on conviction to a fine not exceeding ***two million pounds*** or three times the value of undue advantage received, whichever is greater, or for a term of imprisonment not ***exceeding ten years.***

(2) A person who performs the acts described under subsection (1)—

(a) for wrongful gain;

(b) for wrongful loss to another person; or

(c) for any benefit for oneself or for another person,

is liable on conviction, to a fine not exceeding **three million pound** or to a term of imprisonment not **exceeding five years.**

CHAPTER IV

ESTABLISHMENT OF PROSECUTION UNIT AND PROCEDURAL POWERS OF INVESTIGATIONS

44. The National Cybercrime Prosecution Unit.

(1) There is established the National Cybercrime Prosecution Unit which shall be a unit under the Ministry responsible for Justice and Constitutional Affairs.

(2) The National Cybercrime Prosecution Unit is the competent authority to investigate and prosecute cybercrimes and other violations of the Act;

(3) The Nation Cybercrime Prosecution Unit shall provide assistance in respect of —

(a) the expeditious preservation of data and evidence;

(b) information on the detection of suspects and related matters;

(c) issuing and promulgating guidelines, advisories, and procedures in all matters related to cybercrime investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices;

(d) prescribing forms and templates, including, but not limited to, those for preservation orders, chain of custody, consent to search, consent to assume account/online identity, and request for computer forensic examination.

(4) The Minister shall by regulation, prescribe the composition, qualifications and staff requirements of the Unit.

45. Expedited preservation and partial disclosure of traffic data.

(1) Where the investigatory authority has reasonable grounds to believe that—

(a) any specified traffic data stored in any computer system or device, or by means of a computer system, is reasonably required for the purpose of a criminal investigation; and

(b) there is a risk that the traffic data may be modified, lost, destroyed or rendered inaccessible.

the investigatory authority shall serve a notice on the person who is in possession or control of the traffic data, requiring the person to—

(i) undertake expeditious preservation of such available traffic data regardless of whether one or more service providers were involved in the transmission of that communication; or;

(ii) disclose required traffic data concerning that communication in order to identify the service providers and the path through which communication was transmitted.

(2) The data specified in the notice referred to in subsection (1) shall be preserved and its integrity shall be maintained for a period not exceeding 90 days.

46. **Production Order.**

(1) Where the disclosure of data is required for the purpose of a criminal investigation or prosecution of an offence, the investigatory authority may make an application to the Court for an order compelling—

(a) a person in South Sudan to submit specified data in that person's possession or control, which is stored in a computer system or device;

(b) any service provider offering its services in South Sudan to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material, to which an investigation relates, consists of computer data stored in a computer system, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is easily understood.

47. **Powers of access, search and seizure for purpose of investigation.**

(1) Where the investigatory authority has reasonable grounds to believe that—

(a) stored data is relevant for the purpose of an investigation or the prosecution of an offence, it may make an application to court for the issue of a warrant to enter any premises to access, search and seize such data;

(b) data sought is stored in another computer system or part of it in South Sudan territory, and such data is lawfully accessible from or available to the initial system, the investigatory authority shall expeditiously extend the search or similar access to the other system.;

(2) The investigatory authority may, in the execution of a warrant under subsection (1)

(a) seize or secure a computer system or part of it or a computer data storage medium;

(b) make and retain a copy of those computer data;

(c) maintain the integrity of the relevant stored computer data;

(d) conduct forensic analysis or examination of the computer data storage medium;

(e) render inaccessible or remove those computer data from the accessed computer system.

(3) The investigatory authority may order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs (1) and (2).

48. **Real-time collection of traffic data.**

(1) Where the investigatory authority has reasonable grounds to believe that traffic data is relevant for the purpose of investigation and prosecution of an offence, it may make an application to the Judge in Chambers for an order —

(a) authorising the collection or recording of traffic data on South Sudan territory by technical means, in real-time, associated with specified communications transmitted by means of any computer system;

(b) compelling a service provider, within its technical capabilities, to;

(i) effect such collection and recording specified in paragraph (a); or

(ii) cooperate with the investigatory authority to effect such collection and recording; or

(c) compelling a service provider to keep confidential the fact of the execution of any power provided under this section and any information relating to it.

49. **Interception of content data.**

(1) Where the investigatory authority has reasonable grounds to believe that any content data is relevant for the investigation and prosecution of an offence, it may make an application to the court for an order to—

(a) collect or record content data in the territory of South Sudan by technical means in real-time of specified communications by means of a computer system;

(b) compel a service provider, within its existing technical capabilities, to—

(i) collect or record by technical means in South Sudan;

(ii) cooperate and assist the investigatory authority in the collection or recording of content data, in real-time, of specified communications in South Sudan, transmitted by means of a computer system; or

(c) compel a service provider to keep the confidentiality of the fact of the execution of any power provided for in this section and any information relating to it.

50. **Deletion order.**

(1) The Court may, for the purpose of this Act, upon application by the investigatory authority, and upon being satisfied that a computer system or any other device contains any unlawful material or activity, order that such computer data be

(a) no longer stored on and made available through the computer system or any other device; or

(b) deleted or destroyed.

51. **Limited use of disclosed computer data and information.**

(1) Computer data obtained under this Act by any person authorised, in writing, by the investigatory authority shall be used for the purpose of a criminal investigation or the prosecution of an offence, unless such computer data is sought in—

(a) accordance with any other law;

(b) compliance with an order from a Court;

(c) relation to the prevention of injury or other damage to the health of a person or serious loss of, or damage to, property; or

(d) the public interest.

(2) Subject to subsections (1) and (3), any person authorised by the investigatory authority shall, on receipt of a request, in writing, permit a person who had the custody or control of a computer system to access and copy computer data on the computer system.

(3) A person authorised, in writing, by the investigatory authority, may refuse to give access to computer data or provide copies of such computer data if he has reasonable grounds to believe that—

(a) possession of the data constitutes, or may lead to, or assist in, a criminal offence; or

(b) in connection with which the search was carried out, another ongoing investigation, or any criminal proceedings that are pending or which may be brought in relation to any of those investigations.

CHAPTER V

CRITICAL NATIONAL INFRASTRUCTURE

52. Designation of critical infrastructure.

(1) The Minister may, on the advice of the Authority, designate a computer system or computer network as a critical infrastructure if the Minister considers that the computer system or computer network is essential for—
(a) national security, or

(b) the economic and social well-being of citizens.

(2) Where the Minister designates a computer system or computer network as a critical infrastructure, the Minister shall publish the designation in the *Gazette*.

(3) The Minister shall, in making a determination under subsection (1), consider if the computer system or computer network is necessary for—

(a) the security, defence or international relations of the country;

(b) the production, preservation or identity of a confidential source of information related to the enforcement of criminal law;

(c) the provision of services directly related to—

(i) communications and telecommunications infrastructure;

(ii) banking and financial services;

(iii) public utilities;

(iv) public transportation; and

(v) public key infrastructure;

(d) the protection of public safety and public health, including systems related to essential emergency services;

(e) an international business or communication affecting a citizen of South Sudan or any other international business in which a citizen of South Sudan or the Government has an interest; or

(f) the Legislature, Executive, Judiciary, Public Services or security agencies.

(4) The Minister shall, by publication in the *Gazette*, establish the procedure for the regulation of a critical infrastructure.

53. Registration of critical infrastructure.

(1) The Authority shall register a critical infrastructure.

(2) The Authority shall, by publication, determine –

(a) the requirements for the registration of a critical infrastructure;

(b) the procedure for the registration of a critical infrastructure; and

(c) any other matter relating to the registration of a critical infrastructure.

(3) Where there is any change in the legal ownership of a registered critical infrastructure, the owner of the registered critical infrastructure shall, within seven days after the change, inform the Authority of the change in ownership.

(4) An owner of a registered critical infrastructure who contravenes subsection (3) is liable to pay to the Authority the administrative penalty prescribed by the Minister.

54. **Withdrawal of designation of critical infrastructure.**

The Minister may, on the advice of the Authority and by publication in the *Gazette*, withdraw the designation of a critical infrastructure at any time if the Minister considers that the computer system or computer network no longer satisfies the criteria of a critical infrastructure.

55. **Management and compliance audit of critical infrastructure.**

(1) The Minister shall prescribe minimum standards for prohibitions in respect of the general management of a critical infrastructure that the Minister considers necessary for the protection of national security.

(2) The Authority shall carry out a periodic audit and inspection on a critical infrastructure to ensure compliance with the provisions of this Act.

56. **Duty of owner of critical infrastructure.**

(1) An owner of a critical infrastructure shall—

(a) report a cybersecurity incident within twenty-four hours after the incident is detected to the Authority.

(b) cause an audit to be performed on a critical infrastructure; and

(c) submit a copy of the audit report to the Authority.

(2) An owner of a critical infrastructure who contravenes the provisions of sub section (1), is liable to pay to the Authority the administrative penalty that may be prescribed by the Minister.

57. **Access to critical infrastructure.**

(1) A person shall not without authorisation—
(a) secure access, or

(b) attempt to secure access to a computer system or a computer network designated as a critical infrastructure.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not exceeding one million pounds or to a term of imprisonment of exceeding five years, or to both.

(3) Where the offence committed under subsection (1) —
(a) results in a serious bodily injury, financial loss or damage to the computer system or computer network designated as a critical information infrastructure, the person who committed the offence—

(i) in the case of an individual, is liable on conviction, to a fine not exceeding ***two million*** pounds or to a term of imprisonment not exceeding ***fifteen years*** or to both;

(ii) in the case of a body corporate, a partnership or a firm is liable on conviction to a fine of exceeding ten million pounds; and

(b) is deemed to be a terrorist act, the person who committed the offence is liable on conviction to a term of imprisonment of not exceeding twenty-five years.

(4) Where an offence under subsection (3) is committed by a body corporate or by a member of a partnership or other firm, every director or officer of that body corporate or a member of the partnership or any other person concerned with the management of the firm is deemed to have committed that offence and is liable on conviction, to a fine not exceeding three million pounds.

(5) A person shall not be convicted of an offence by virtue of subsection (4) if it is proved that—

(a) due diligence was exercised to prevent the commission of the offence; and

(b) the offence was committed without the knowledge, consent or connivance of that person.

58. Responsibility of the Authority Relating to Response to Cybersecurity Incident

(1) The Authority shall establish a national computer incident response team coordination centre (SS-CIRT/CC) to serve as a point of contact to identify, defend, respond and resolve cybersecurity incidents;

(2) The cybersecurity coordination centre (SS-CIRT/CC) shall serve as the focal point for all instances of cybersecurity incidents by:

(a) providing technical analysis of computer security incidents;

(b) conducting awareness campaigns and training programs, empowering individuals, and organizations with the knowledge to protect themselves against cyber threats;

(c) issuing relevant alerts and advisories on emerging threats to computer security thus helping individuals and organizations enhance their cybersecurity posture;

(d) providing timely, actionable insights into emerging threats and vulnerabilities;

(e) coordinating cyber security incident responses with trusted third parties.

(3) The cybersecurity coordination centre shall establish a cybersecurity incident reporting and information sharing platform to enable public to report a cybersecurity incident.

CHAPTER VI

INTERNATIONAL COOPERATION

59. International co-operation.

(1) The Authority shall in the performance its functions, promote the security of cyberspace through international co-operation.

(2) The Authority shall implement relevant measures for the effective implementation and enforcement of international treaties on cybercrime and cybersecurity, of which South Sudan is a signatory.

60. General Principles Relating to International Cooperation.

(1) The Authority may make a request for mutual legal assistance in any criminal matter to a foreign State for the purpose of—

(a) undertaking investigations or proceedings concerning offences related to computer systems, electronic communications or computer data;

(b) collecting evidence of an offence in electronic form;

(c) collecting evidence in electronic form of any criminal offence not limited to offences under this Act; or

(d) obtaining expeditious preservation and disclosure of data, including traffic data, real-time collection of traffic data associated with specified communications or interception of computer data or any other means, power, function or provisions under this Act.

(2) For any of the purposes listed in subsection (1)(a) to (d), a requesting State may make a request for mutual legal assistance to the Authority in any criminal matter.

(3) Where a request is received under subsection (2), the Authority may, subject to this Act and any other relevant law grant the legal assistance requested.

(4) The Authority may require a requesting State to—

(a) keep the contents, information and materials provided in a confidential manner;

(b) only use the contents, information and materials provided for the purpose of the criminal matter specified in the request; and

(c) use the contents, information and materials subject to such conditions as may be specified.

(5) Prior to providing any information, the Authority may request that it be kept confidential or only used subject to such conditions as may be specified.

(6) If the receiving Party cannot comply with such a request, it shall notify the Authority accordingly, which shall then determine whether the information should nevertheless be provided.

(7) Where, subject to subsections (5) and (6), a receiving party accepts the information, it shall comply with the conditions specified.

61. **Spontaneous information**

(1) The Authority may, subject to this Act and any other relevant law, without a prior request, forward to a foreign State information obtained within the framework of a South Sudan investigation where it considers that the disclosure of such information may—

(a) assist the foreign State in initiating or carrying out investigations or proceedings concerning criminal offences related to cybercrime and cybersecurity; or

(b) lead to a request for cooperation by the foreign State under this Act.

(2) Prior to providing the information under subsection (1), the Authority may request that such information be kept confidential or disclosed only subject to such conditions as may be specified.

(3) Where a foreign State does not comply with the conditions specified under subsection (2), the State shall forthwith notify the Authority.

(4) The Authority shall, on receipt of a notice under subsection (3), determine whether the foreign State should be provided the information requested for.

(5) The Authority may refuse to provide the information where the foreign State does not take the commitment to respect the conditions specified by the Authority.

62. **Expedited preservation of stored computer data.**

(1) A requesting State which intends to make a request for mutual legal assistance for the search or similar access, seizure or similar securing or the disclosure of computer data, may request the Authority to obtain the expeditious preservation of stored computer data located within the territory of South Sudan.

(2) The requesting State shall, in its request under subsection (1), specify—

(a) the name of the authority seeking the preservation;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the stored computer data to be preserved and its connection to the offence;

(d) any available information identifying the custodian of the stored computer data or the location of the computer system;

(e) the necessity of the preservation; and

(f) the intention to submit a request for mutual assistance for the search or similar access, seizure or similar securing or the disclosure of the stored computer data.

(3) The Authority shall-

(a) on receipt of the request under this section, take appropriate measures to preserve the specified data in accordance with the procedures set out in, and powers conferred under, this Act and any other relevant legislation.

(b) The purpose of the preservation of stored computer data effected under this section shall be to enable the State to submit a

request for the search or access, seizure or securing, or the disclosure of the data.

(c) The stored computer data shall be preserved for a period not exceeding 120 days.

(4) The data shall, on receipt for a request under this section, continue to be preserved pending the final decision being made with regard to that request.

63. **Expedited disclosure of preserved traffic data.**

(1) Where, in the course of executing a request under section 48 with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Authority shall expeditiously disclose to the requesting State a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

(2) Disclosure of traffic data under subsection (1) may only be withheld if the Authority considers that the execution of the request is likely to prejudice South Sudan's sovereignty, security, public order or public interest.

64. **Mutual assistance regarding accessing of stored computer data.**

(1) A requesting State may request the Inspector General of Police, through the Authority, to search or similarly access, seize or similarly secure, and disclose stored computer data located within South Sudan, including computer data that are specified in section 48.

(2) For the purpose of subsection (1), the requesting State shall—

(a) provide the name of the authority conducting the investigation or proceedings to which the request relates;

(b) give a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;

(c) give a description of the purpose of the request and the nature of the assistance being sought;

(d) in the case of a request to restrain or confiscate assets believed, on reasonable grounds, to be located in South Sudan, give details of the offence, particulars of the investigation or proceedings commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order;

(e) give details of any procedure that the requesting State wishes to be followed by South Sudan in giving effect to the request, particularly in the case of a request to take evidence;

(f) include a statement setting out any demands of the requesting State concerning any confidentiality relating to the request and the reasons for those demands;

(g) give details of the period within which the requesting State wishes the request to be complied with;

(h) where applicable, give details of the property, computer system or device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in South Sudan;

(i) give details of the stored computer data, or program to be seized and its relationship to the offence;

(j) give any available information that may identify the custodian of the stored computer data or the location of the computer system or device;

(k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and

(l) give any other information that may assist in giving effect to the request.

(3) The Authority shall, on receiving the request under this section, take such appropriate measures as may be required to obtain necessary authorisation, including any warrants, to execute the request in accordance with this Act and any other relevant law.

(4) Where the Authority obtains the necessary authorisation in accordance with subsection (3), including any warrants, to execute the request, the Authority may seek the support and cooperation of the requesting State during such search and seizure.

(5) For the purpose of conducting the search and seizure request, the Authority shall, provide, to the requesting State, the results of the search and details in respect of any electronic or physical evidence seized.

(6) The request shall be responded to on an expedited basis where—

(a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

(b) any relevant laws so require.

65. **Trans border access to stored computer data with consent or where publicly available.**

The investigatory authority may, without the authorisation of another State, and subject to this Act—

(a) access publicly available stored computer data, regardless of where the data is located geographically; or

(b) access or receive, through a computer system in South Sudan, stored computer data located in another State, if a police officer or authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to South Sudan through that computer system.

66. Mutual assistance in real-time collection of traffic data.

(1) A requesting State may request the Authority to provide assistance in real-time collection of traffic data associated with specified communications in South Sudan, transmitted by means of a computer system.

(2) For the purpose of subsection (1), the requesting State shall specify —

(a) the authority seeking the use of powers under this section;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the name of the authority which has access to the relevant traffic data;

(d) the location at which the traffic data may be held;

(e) the intended purpose of requiring the traffic data;

(f) such information as may be required to identify the traffic data;

(g) any further details relevant to the traffic data;

(h) the reason for using powers under this section; and

(i) the terms and conditions for the use and disclosure of the traffic data to third parties.

(3) The Authority shall, on receipt of the request under this section, take all appropriate measures to obtain necessary authorisation, including any warrant to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.

(4) Where the Authority obtains the necessary authorisation, including any warrant to execute upon the request, the Authority may seek the support and cooperation of the requesting State during the collection.

(5) The Authority shall, upon conducting the measures under this section, and subject to section 51 provide the results to the requesting State.

67. **Mutual assistance regarding interception of content data.**

(1) A requesting State may request the Authority to provide assistance in the real-time collection or recording of content data of specified communications in South Sudan transmitted by means of a computer system.

(2) When making a request under subsection (1), a requesting State shall specify —

(a) the authority seeking the use of powers under this section;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the name of the authority with access to the relevant communication;

(d) the intended duration of the interception;

(e) the reason for using powers under this section; and

(f) the terms and conditions of the use and disclosure of the communication to third parties.

(3) The Authority shall, on receipt of the request under this section, take appropriate measures as may be required to obtain necessary authorisation, including any warrant to execute the request in accordance with this Act and any other relevant legislation.

(4) Where Authority obtains the necessary authorisation, including any warrant to execute upon the request, the Authority may seek the support and cooperation of the requesting State during the interception.

(5) The Authority shall, upon conducting the measures under this section, provide the results to the requesting State.

CHAPTER VII

GENERAL PROVISIONS.

68. **Co-operation.**

A public institution or a private institution shall co-operate with the Authority for the purpose of ensuring the cybersecurity of the country.

69. **General Penalty.**

A person who contravenes a section of this Act for which a penalty is not provided commits an offence and is liable on conviction to a fine of exceeding than one million pounds or to a term of imprisonment of not exceeding five years, or to both.

70. Guidelines.

The Authority shall publish guidelines that the Authority considers necessary for—

(a) the identification of critical infrastructure;

(b) the registration of critical infrastructure;

(c) the protection of critical infrastructure;

(d) the management of critical infrastructure;

(e) access to, transfer and control of data in critical information infrastructure;

(f) the storage or archiving of data or information in critical infrastructure;

(g) reporting incidents involving critical infrastructure; and

(h) any other matter required for the adequate protection of critical infrastructure.

71. Directives.

(1) The Authority may issue directives to an owner of a critical infrastructure, a cybersecurity service provider or service provider for the purpose of ensuring the cybersecurity of the country.

(2) An owner of a critical information infrastructure, a cybersecurity service provider or a service provider who fails to comply with the directives issued under subsection (1) is liable to pay to the Authority the administrative penalty prescribed under this Act.

72. Administrative penalties for contraventions.

The Authority shall, for the purpose of imposing an administrative penalty under this Act, take into account –

(a) the size of the service provider concerned;

(b) the criticality of the sector;

(c) the impact of the contravention; and

(d) any other relevant criterion that the Minister may determine.

73. Regulations.

The Minister may make regulations to provide for-

(a) the forms for applications;

(b) authorisations and licences;

(c) the use of equipment to intercept or disable a digital technology service or product by authorised persons to execute an interception warrant;

(d) accreditation of cybersecurity professionals and practitioners;

(e) the operationalisation of a platform for cross-sector engagement on matters of cybersecurity for effective coordination and cooperation between key public institutions and the private sector;

(f) the promotion and development of cybersecurity to ensure a secured and resilient digital ecosystem;

(g) certification of cybersecurity products and technology solutions;

(h) implementation of early warning system;

(i) receipt of complaints by the Authority from cybersecurity service providers, licensed institutions, the public and other similar international bodies;

(j) the modalities for—

(i) the preservation of data; and
(ii) the retention of data;

(k) dispute resolution;

(l) administrative penalties provided for in this Act; and

(m) any other matters necessary for the effective implementation of this Act.

74. **Extradition.**

Any offence under this Act is an extraditable crime for which extradition may be granted or obtained under the applicable law for extradition**.**

75. **Forfeiture.**

The Court before which a person is convicted of an offence may, in addition to any other penalty imposed, order the forfeiture of any apparatus, article or device which is the subject matter of the offence or is used in connection with the commission of the offence.

Issued Under my Hand in Juba, this ……Day of the Month of ……in the Year 2024.

Salva Kiir Mayardit
President

Republic of South Sudan
JUBA

_____