LAWS OF SOUTH SUDAN

CYBERCRIMES AND COMPUTER MISUSE PROVISIONAL ORDER, 2021

LAWS OF SOUTH SUDAN

CYBERCRIMES AND COMPUTER MISUSE PROVISIONAL ORDER, 2021

Table of Content

Arrangement of Chapters

21. Spamming
22. Phishing
23. Pornographic Content
24. Sexual Communication
25. Offensive Communication
26. Cyberstalking
27. Cybersquatting
28. Offenses Related to Electronic Messages
29. Cyberterrorism
30. Human Trafficking
31. Drug Trafficking
32. Espionage
33. Economic Sabotage
34. Hacking Critical Infrastructure or a Computer System
35. Regulations

CYBERCRIMES AND COMPUTER MISUSE PROVISIONAL ORDER, 2021

In exercise of the powers conferred upon me in Article 86 (1) of The Transitional Constitution of South Sudan, 2011(as amended), I, do hereby issue the following:

CHAPTER I

PRELIMINARY PROVISIONS

1. Title and Commencement

This Provisional Order shall be cited as "The Cybercrimes and Computer Misuse Provisional Order, 2021" 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Any legislation governing the subject of this Provisional Order is hereby repealed; provided that, all actions taken, proceedings, appointments, orders and regulations made or issued thereunder shall remain in force until they are repealed or amended in accordance with the provisions of this Provisional Order.

3. Purpose

The purpose of this Provisional Order is to protect and prevent any crimes committed through computer or computer system, Internet or any related activities.

4. Authority and Application

(1) This Provisional Order 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 Provisional Order shall apply to all cybercrimes and computer misuse committed in or outside the Republic of South Sudan.

5. Interpretations

In this Provisional Order, unless the context otherwise requires:

"Access" means gaining entry into or intent to gain entry by a person to a program or data stored in a computer system and the person either:

(a) alters, modifies, erases a program, data or any aspect related to the program or data in the computer system;
(b) copies, transfers, moves a program or data to:

(i) any computer system, device or storage medium other than that in which it is stored; or

(ii) a different location in the same computer system, device or storage medium in which it is stored.

(c) causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner; or

(d) uses it by causing the computer to execute a programme or is itself a function of the program;

"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;

"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;

"Competent Minister" means the Minister responsible for communication;

"Computer Misuse" means any use of computer, device, information system for:

(a) what it was not intended to do;

(b) to commit any crime;

(c) to aid in committing a crime;

(d) furtherance of a crime;

(e) to alert normal functioning of a computing device, network or any information system asset.

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

"Cybersecurity" means ensuring confidentiality, integrity and availability of information systems in relation to the cyberspace;

"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 organized 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 field of digital forensics by training, practice, experience, certification, formal education on digital forensics or other qualifications;

"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;

"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 organization 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 document 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" 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;

"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;

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

"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;

"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;

"Publish" means 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;

"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;

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

"Traffic Data" means computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communications origin, destination, route, time, date, size, duration or the type of underlying service;

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

"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 organization.

CHAPTER II

OBLIGATIONS OF SERVICE PROVIDER AND JURISDICTION OF CYBERCRIMES AND COMPUTER MISUSE

6. Obligations of Service Provider

(1) Without prejudice to the National Communication Act, a service provider shall:

(a) keep, store, record information system or any means of information technology for continuous period of 180 days, the data to be saved include following:

(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 for any communication;

(iv) any other data specified by the National Communication Authority.

(b) take reasonable steps to inform its clients of cybercrimes trends which affect or may affect its clients;

(c) disclose abuses to the concerned victim and to relevant authorities that infractions are committed;

(d) maintain confidentiality of the data saved and stored and not disclosing them without an order from competent judicial authority, this includes:

(i) personal data of any user of these services or any data or information related to the consent and the provided account that this users or persons entered into communication with;

(ii) securing data and information in a way that preserves its biography and not penetrating or damaging it;

(2) Without prejudice to the privacy guaranteed by the Constitution, service provider and its agents are obliged to comply with relevant law enforcement agencies in accordance with technical capabilities in allowing operation of the law.

(3) Without prejudice to the provisions of Consumer Protection Act, the service provider shall provide its users and specialized 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 service provider;

(b) any other information that the National Communication Authority considers important for the protection of users.

7. Jurisdiction of Cybercrimes and Computer Misuse

Without prejudice to the provisions of the Penal Code, the provisions of this Provisional Order shall apply to a crime committed in or outside the country, which occurs in the following cases:

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

ESTABLISHMENT, POWERS AND FUNCTIONS OF THE INVESTIGATING AUTHORITIES AND INTERNATIONAL COOPERATION

8. Establishment of Specialized Prosecution Unit

The Minister of Justice may establish a specialized public prosecution attorney unit to investigate and prosecute cybercrime offences under this Provisional Order.

9. Powers and Functions of the Investigating Authorities

Notwithstanding the provisions of the Code of Criminal Procedure, the investigating authorities shall exercise and perform the following:

(1) Seize, withdraw, collect, preserve data and information system or tracking them in any place they are located, and the digital evidence is delivered to the investigating authority, provided that it shall not affect the continuity of the network system and provision of service as it may be necessary.

(2) Access, inspect, search to conduct digital forensic into the computer programme, and other devices of information system.

(3) Order the service provider to handover data or information related to information system or device.

10. Use of Forensic Tools

(1) The use of forensic tool shall be authorised by competent court through an application, when an investigating authority determines that an essential evidence shall not be collected under this section.

(2) The application under subsection (1) of this Section shall contain:
(a) the name and address of the suspect;
(b) a description of the targeted device, computer system; and
(c) a description of the intended measures, purpose, extent and duration of the utilization.

(3) The investigating authority shall ensure that any modification made to the computer system or computer data of the suspect are limited to the investigation and that any changes reversed after the completion of the investigation is restored into the system.

(4) During investigation, the investigating authority shall log:
(a) the technical means used, time and date of the application;
(b) the identification of the computer system and details of the modification undertaken within the investigation;
(c) any information obtained.

(5) The information obtained under this section shall be protected against any modification, unauthorized deletion and unauthorized access.

(6) The authorization under this section shall be valid for a period of fifteen days.

(7) The court may, on application, extend the period under subsection (6) of this Section for a further period of fifteen days or to such other period as it deems necessary.

(8) Where the installation process requires a site visit, the requirements of Section 9 of this Section shall apply.

(9) In addition to the order granted under subsection (1) of this Section, the court may, on application, order the service provider to support the installation process of the forensic tool.

(10) Extraction, processing and presentation of digital evidence shall be conducted by digital forensic expert.

11. International Cooperation in Combating Cybercrimes and Computer Misuse

Any country requesting lawful assistance from the Republic of South Sudan on matters in this Provisional Order, shall be through regional, international agreements ratified by the Republic of South Sudan or bilateral, multilateral agreements and application of the principles of reciprocity by exchanging information in accordance with the mutual legal assistance on the basis of uniform or reciprocal manner.

CHAPTER IV

OFFENCES AND PENALTIES

12. Unauthorized Data Transmission

Whoever:

(a) communicates, discloses or transmits any 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.

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

13. Unauthorized Device

Whoever knowingly:

(a) manufactures, adapts, sells, procures for use, imports, offers to supply, distributes a device, program, computer password, access code or similar data designed or adapted primarily for the purpose of committing unlawful act;
(b) receives, or is in possession of, a program, a computer password, device, access code, or similar data from any action specified under subsection (a) of this Section and intends that it be used to commit or assist in commission of an offence.

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

14. Disclosure of Password or Data

Whoever discloses any password, access code or any other means of gaining access to any programme, data or computer system.
Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding ten years or a fine or both.

15. Offences Committed by Means of Information Systems and Technologies

Whoever fraudulently uses the computer network and information technology with intent to access to numbers, data, bank card services or any electronic payment tools to obtain financial gains or any other services.
Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding three years or a fine or both.

16. Impersonation and Other Identity Related Offences

Whoever:

(a) intentionally uses somebody identity over the internet in bad faith to profit, mislead or destroy reputation, if such identity is similar, undistinguishable, or confusingly similar to an existing name or description that belongs to another person or organ;

(b) knowingly or wilfully, while not being a manufacturer of a computer system or an authorized agent of the manufacturer, changes computer system equipment identity or the process of accessing to it;

(c) fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person.

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

17. Offences against the Integrity of Computer or Information Systems

Whoever commits an act which causes directly or indirectly a degradation, failure, interruption or obstruction of the operation of a computer or computer system, or a denial of access, damage of any program or data stored in the computer system.
Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding three years or a fine or both.

18. Publication of Indecent Content and Privacy

Whoever:

(a) publishes, transmits or causes to be published any indecent message using a computer or a computer system;

(b) prepares using information network, communication, any means of information communication or application with intent to violate privacy of any person or interfering in his or her private affairs or family life, by photographing, special writing, dissemination of pictures of interception, tapping, viewing such person correspondence, receiving, publishing any information about such person.

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

19. Publication of False Information

Whoever publishes false, deceptive, fictitious, misleading or inaccurate information or data presented in a picture, text, symbol or any other form in a computer system with intent to defame, threaten, abuse, insult, deceive or mislead the public.
Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding five years or a fine or both.

20. Incitement Through Computer Systems

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

21. Spamming

Whoever intentionally sends unsolicited messages repeatedly or to a large number of persons by use of a computer or a computer system after receiving a message, uses a computer or a computer system to retransmit such a message to many.
Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding five years or a fine or both.

22. Phishing

Whoever establishes and uses a website or sends an electronic message using a computer or a computer system in order to have access to confidential information from a visitor of the website or recipient of the message with intent to use them for unlawful purposes of stealing information or obtaining unauthorized access to a computer or a computer system.
Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding five years or a fine or both.

23. Pornographic Content

Whoever:

(a) publishes or causes to be published, makes available, facilitates the access of material, content of pornographic nature through a computer system or through any other means of information communication technology;
(b) publishes or causes to be published, makes available, facilitates the access of pornography which is lascivious or obscene;
(c) publishes child pornography, makes available, facilitates the access of child pornography through a computer or a computer system;

(d) 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.

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

24. Sexual Communication

Whoever intentionally communicates with a child using a computer or a computer system to send sexual related messages to encourage or engage in sexual activities.
Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding ten years or a fine or both.

25. Offensive Communication

Whoever intentionally uses electronic communication to disrupt or attempts to disturb legitimate communication whether or not a conversation ensues.
Commits an offence and upon conviction shall be sentenced to imprisonment to a term not exceeding four years or a fine or both.

26. Cyberstalking

Whoever 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.

27. Cybersquatting

Whoever 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.

28. Offenses Related to Electronic Messages

Whoever:

(a) misdirects electronic messages;
(b) induces any person in charge of electronic devices to deliver any electronic messages not specifically meant for him or her;
(c) intentionally 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;
(d) unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed;

(e) 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;
(f) knowingly and without authority causes any loss of property to another by altering, erasing, inputting or suppressing any data stored in a computer;
(g) sends an electronic message which materially misrepresents any fact upon which reliance by another person is caused to suffer any damage or loss;
(h) with intent to defraud, franks electronic messages, instructions, subscribes any electronic messages or instructions; or
(i) 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 to a fine or both.

Offences that Threaten National Security and Other Serious Crimes

29. Cyberterrorism

Whoever:
(a) establishes, helps to establish, publishes, attempts or uses a site of a terrorist group using Internet, a computer or a computer system in order to facilitate communication by its leadership; or
(b) accesses or causes to be accessed a computer or computer system or network for purposes of carrying out a terrorist act.

Commits an offence and upon conviction shall be sentenced to imprisonment for a term not less than twenty-five years or a fine or both.

30. Human Trafficking

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.

31. Drug Trafficking

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.

32. Espionage

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

33. Economic Sabotage

Whoever 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, 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.

34. Hacking Critical Infrastructure or a Computer System

Whoever undertakes hacking activities with intention to access critical data, knowingly damage, paralyse or interfere with critical infrastructure or a computer system to defraud, obtain information or any other related activities.
Commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding fifteen years or a fine or both.

35. Regulations

The Competent Minister responsible for communication may issue rules and regulations for effective and efficient implementation of this Provisional Order.

Issued under my hand and the Seal of the Republic in Juba this..7th..
Day of the Month of May in the Year 2021.

Salva Kiir Mayardit
President,
Republic of South Sudan
Juba.