THE CYBERCRIMES ACT, 2015

ARRANGEMENT OF SECTIONS

Section *Title*

PART I
PRELIMINARY PROVISIONS

PART II
PROVISIONS RELATING TO OFFENCES AND PENALTIES

PART V
LIABILITY OF SERVICE PROVIDERS

PART VI
GENERAL PROVISIONS

PART VII
CONSEQUENTIAL AMENDMENTS

(a) Amendment of the Electronic and Postal Communications Act No.3 of 2010.

(b) Amendment of the Penal Code, Cap.16

(c) Amendment of Anti-Money Laundering, Cap.423

(d) Amendment of the Extradition Act, Cap.368

THE UNITED REPUBLIC OF TANZANIA

NO.14 OF 2015

I ASSENT,

.....

President

25th April, 2015

An Act to make provisions for criminalizing offences related to computer systems and Information Communication Technologies; to provide for investigation, collection, and use of electronic evidence and for matters related therewith.

ENACTED by Parliament of the United Republic of Tanzania.

PART I
PRELIMINARY PROVISIONS

Short title and commencement

1. This Act may be cited as the Cybercrimes Act, 2015 and shall come into operation on such date as the Minister may, by Notice published in the *Gazette* appoint.

Application

2. Save for section 50, this Act shall apply to Mainland Tanzania as well as Tanzania Zanzibar.

Interpretation

3. In this Act, unless the context otherwise requires-

"access" in relation to any computer system, means entry to, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system or network or data storage medium;

"access provider" means a person who provides electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network;

"caching provider" means a person who provides an electronic data transmission service by automatic, intermediate or temporary storing information, for the purpose of making more efficient the information's onward transmission to other users of the service upon their request;

"child" means a person below the age of eighteen years;

"child pornography" means pornographic material that depicts presents or represents:

(a) a child engaged in a sexually explicit conduct;

(b) a person appearing to be a child engaged in a sexually explicit conduct; or

(c) an image representing a child engaged in a sexually explicit conduct;

"computer system" means a device or combination of devices, including network, input and output devices capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that perform logic, arithmetic data storage and retrieval communication control and other functions;

"computer data" means any representation of facts, concepts, information or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"data storage medium" means any device, article or material from which computer data or information is capable of being stored or reproduced, with or without the aid of any other device or material;

"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;

"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 or in any other similar form;

"forensic tool" means an 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 which includes keystroke logging or collection of investigation information about a uses of the computer or computer system;

"hinder" in relation to a computer system includes -

(a) causing electromagnetic interference to a computer system;

(b) corrupting a computer system by any means; or

(c) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;

"hosting provider" means a person who provides an electronic data transmission service by storing information provided by a user of the service;

"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;

"intellectual property rights" means the rights accrued or related to copyright, patent, trade mark and any other related matters;

"interception" in relation to a function of computer, includes acquiring, viewing, listening or recording any computer data communication through any other means of electronic or other means, during transmission through the use of any technical device;

"law enforcement officer" means a police officer of the rank of Assistant Inspector or above or an investigator of equivalent rank of inspector and above, member of Tanzania Intelligence Service, prosecutor, or any authorized officer of the authority responsible for communication or any other person authorised in any written law;

"Minister" means the Minister for the time being responsible for Information and Communication Technology;

"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;

"property" means property of any kind, whether movable or immovable, tangible or intangible, and includes-

(a) any currency either as a legal tender in the United Republic of Tanzania or not;

(b) information, including an electronically produced program or data or copy thereof, human or computer-readable data; or

(c) any right or interest in property;

"racist and xenophobic material" means any material which advocates, promotes or incites hatred, discrimination or violence, against any person or group of persons based on race, colour, descent, national or ethnic origin or religion;

"service provider" means a person or party that makes information system services available to third parties;

PART II
PROVISIONS RELATING TO OFFENCES AND PENALTIES

Illegal access

4.-(1) A person shall not intentionally and unlawfully access or cause a computer system to be accessed.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine of not less than three million shillings or three times the value of the undue advantage received, whichever is greater or to imprisonment for a term of not less than one year or to both.

Illegal remaining

5.-(1) A person shall not intentionally and unlawfully, remain in a computer system or continue to use a computer system after the expiration of time which he

was allowed to access the computer system.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction to a fine of not less than one million shillings or to imprisonment for a term of not less than one year or to both.

Illegal interception

6.-(1) A person shall not intentionally and unlawfully-

(a) intercept by technical means or by any other means-

(i) a non-public transmission to, from or within a computer system;

(ii) a non-public electromagnetic emission from a computer system;

(iii) a non-public computer system that is connected to another computer system; or

(b) circumvent the protection measures implemented to prevent access to the content of non-public transmission.

(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine of not less than five million shillings or to imprisonment for a term of not less than one year or to both.

Illegal data interference

7.-(1) A person who intentionally and unlawfully-

(a) damages or deteriorates computer data;

(b) deletes computer data;

(c) alters computer data;

(d) renders computer data meaningless, useless or ineffective;

(e) obstructs, interrupts or interferes with the lawful

use of computer data;

(f) obstructs, interrupts or interferes with any person in the lawful use of computer data; or

(g) denies access to computer data to any person authorized to access it,

commits an offence and is liable on conviction, to a fine of not less than ten million shillings or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than three years or to both.

(2) A person who -

(a) communicates, discloses or transmits any computer data, program, access code or command to an unauthorized person;

(b) internationally and unlawfully receives unauthorised computer data,

commits an offence and is liable on conviction, to a fine of not less than two million shillings or three times the value of the undue advantage received, whichever is greater, or to imprisonment for a term of not less than one year or to both.

(3) A person who intentionally and unlawfully destroys or alters any computer data, where such data is required to be maintained by law or is an evidence in any proceeding under this Act by-

(a) mutilating, removing or modifying the data, program or any other form of information existing within or outside a computer system;

(b) activating, installing or downloading a program that is designed to mutilate, remove or modify data, program or any other form of information existing within or outside a computer system; or

(c) creating, altering, or destroying a password, personal identification number, code or method used to access a computer system,

commits an offence and is liable on conviction to a fine of not less than twenty million shillings or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than one year or to both.

Data espionage

Cap. 47

8.-(1) Without prejudice to the National Security Act, a person shall not obtain computer data protected against unauthorized access without permission.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than twenty million shillings or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than five years or to both.

Illegal system interference

9. A person who intentionally and unlawfully hinders or interferes with-

(a) the functioning of a computer system; or

(b) the usage or operation of a computer system,

commits an offence and is liable on conviction, to a fine of not less than two million shillings or three times of value the undue advantage received, whichever is greater, or to imprisonment for a term of not less than one year or to both.

Illegal device

10.-(1) A person shall not unlawfully deal with or possess:

(a) a device, including a computer program, that is designed or adapted for the purpose of

committing an offence;

(b) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed with the intent that it be used by any person for the purpose of committing an offence.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction, to a fine of not less than ten million shillings or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than three years or to both.

Computer-related forgery

11.-(1) A person shall not intentionally and unlawfully input, alter, delay transmission or delete computer data, resulting in unauthentic data, with the intent that it be acted upon as if it were authentic, regardless of whether or not the data is readable or intelligible.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than twenty million shillings or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than seven years or to both.

Computer-related fraud

12.-(1) A person shall not cause a 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,

with fraudulent or dishonest intent.

(2) A person who contravenes subsection (1)

commits an offence and is liable on conviction, to a fine of not less than twenty million shillings or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than seven years or to both.

Child pornography

13.-(1) A person shall not-

(a) publish child pornography, through a computer system; or

(b) make available or facilitate the access of child pornography through a computer system.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction, to a fine of not less than fifty million shillings or three times the value of undue advantage received, whichever is greater, or to imprisonment for a term of not less than seven years or to both.

(3) A person who is convicted for an offence under this section may, in addition to any other punishment, be adjudged to compensate a person injured by the offence.

Pornography

14.-(1) A person shall not publish or cause to be published through a computer system or through any other information and communication technology:

(a) pornography; or

(b) pornography which is lascivious or obscene.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction, in the case of publication of-

(a) pornography, to a fine of not less than twenty million shillings or to imprisonment for a term of not less than seven years or to both; and

(b) pornography which is lascivious or obscene, to a fine of not less than thirty million shillings or to imprisonment for a term of not less than ten years or to both.

Identity related crimes

15. (1) A person shall not, by using a computer system impersonate another person.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction, to a fine of not less than five million shillings or three times the value of undue advantage received by that person, whichever is greater, or to imprisonment for a term of not less than seven years or to both.

Publication of false information

16.- Any person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceiptive, misleading or inaccurate, and with intent to defame threaten, abuse, insult, or otherwise deceive or mislead the public or councelling commission of an offence, commits an offence, and shall on conviction be liable to a fine of not less than five million shillings or to imprisonment for a term of not less than three years or to both.

Racist and xenophobic material

17.-(1) A person shall not, through a computer system -

(a) produce racist or xenophobic material for the purposes of distribution;

(b) offer or make available racist or xenophobic material ; or

(c) distribute or transmit racist or xenophobic material.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than three million shillings or to imprisonment for a term of not less than one year or to both.

Racist and xenophobic motivated insult

18.-(1) A person shall not insult another person through a computer system on the basis of race, colour, descent, nationality, ethnic origin or religion.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than three million shillings or to imprisonment for a term of not less than one year or to both.

Genocide and crimes against humanity

19.-(1) A person shall not unlawfully publish or cause to be published, through a computer system, a material which incites, denies, minimises or justifies acts constituting genocide or crimes against humanity.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than ten million shillings or to imprisonment for a term of not less than three years or to both.

(3) For the purpose of this section, "genocide" shall have a meaning ascribed to it under the Convention on the Prevention and Punishment of the Crime of Genocide, 1948.

Unsolicited messages

20.-(1) A person shall not, with intent to commit an offence under this Act -

(a) initiate the transmission of unsolicited messages;

(b) relay or retransmit unsolicited messages , or

(c) falsify header information in unsolicited messages.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than three million shillings or three times the value of undue advantage received, whichever is greater or to imprisonment for a term of not less than one year or to both.

(3) For the purpose of this section, "unsolicited messages" means any electronic message which is not solicited by the recipient.

Disclosure of details of investigation

21. (1) A person shall not unlawfully disclose details of a criminal investigation, which requires confidentiality.

(2) A person who contravenes subsection (1) commits an offence and, is liable on conviction to a fine of not less than ten million shillings or to imprisonment for a term of not less than three years or to both.

Obstruction of investigation

22.-(1) A person who intentionally and unlawfully destroy, delete, alter, conceal, modify, renders computer data meaningless, ineffective or useless with intent to obstruct or delay investigation commits an offence and on conviction, is liable to a fine of not less than three million shillings or to imprisonment for a term not less than one year or both.

(2) A person who intentionally and unlawfully prevents the execution or fails to comply with an order issued under this Act, commits an offence and is liable, on conviction, to a fine of not less than three million shillings or to imprisonment for a term of not less than one year or to both.

Cyber bullying

23. (1) A person shall not initiate or send any electronic communication using a computer system to another person with intent to coerce, intimidate, harass or cause emotional distress.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than five million shillings or to imprisonment for a term of not less than three years or to both.

Violation of intellectual property rights

24.-(1) A person shall not use a computer system with intent to violate intellectual property rights protected under any written law.

(2) A person who contravenes subsection (1) commits an offence and in case the infringement is on -

(a) non-commercial basis, is liable to a fine of not less than five million shillings or to imprisonment for a term of not less than three years or both; or

(b) commercial basis, is liable to a fine of not less than twenty million shillings or to imprisonment for a term of not less than five years or to both, in addition, be liable to pay compensation to the victim of the crime as the court may deem just.

Principal offenders

25.- (1) Any person who–

(a) does an act or makes an omission which constitutes an offence;

(b) does or omits to do any act for the purpose of enabling or aiding another person to commit an offence;

(c) aids or abets another person in committing an offence;

(d) counsels or procures any other person to commit an offence,

is deemed to have taken part in committing the offence, and shall be charged as a person who committed an offence.

(2) A person who procures another to do or omit to do any act of such a nature that, if he had himself done the act or made the omission, the act or omission would have constituted an offence on his part, commits an offence of the same kind and is liable to the same punishment as if he had himself had done the act or the omission.

Attempt

26.- (1) Where a person, intends to commit an offence, puts his intention into execution by means adapted to its fulfilment, and manifests his intention by some overt act, but does not fulfil his intention to such extent as to commit the offence, he is deemed to have attempted to commit the offence.

(2) For the purposes of this section, it is immaterial-

(a) except so far as regards to punishment, whether-

(i) the offender does all that is necessary on his part for completing the commission of the offence; or

(ii) the complete fulfilment of his intention is prevented by circumstances independent of his will; or

(iii)he desists of his own motion from further execution of his intention;

(b) that by reason of circumstances not known to the offender it is impossible to commit the offence.

(3) A person who attempts to commit an offence under this Act is guilty of an offence and is liable on

conviction to a fine not less than one million shillings or to imprisonment for a term not less than six month or to both.

Conspiracy to commit offence

27. Any person who conspires with another person to commit an offence under this Act, commits an offence, and is liable on conviction to a fine of not less than one million shillings or to imprisonment for a term of not less than one year or to both.

Protection of critical information infrastructure

28.-(1) The Minister may, by order published in the *Gazette*, designate a computer system as critical information infrastructure.

(2) The order under subsection (1) may prescribe guidelines or procedures in respect of-

(a) registration, protection or preservation of critical information infrastructure;

(b) general management of critical information infrastructure;

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

(d) integrity and authenticity of data or information contained in any critical information infrastructure;

(e) methods to be used in the storage or archiving data or information in critical information infrastructure;

(f) disaster recovery plans in the event of loss of the critical information infrastructure or any part of critical information infrastructure;

(g) manner and procedure for carrying out audit and inspection on any critical information infrastructure; and

(h) any other matter that is relevant for adequate

protection, management and control of data and other resources in a critical information infrastructure.

(3) For the purpose of this section, "critical information infrastructure" includes assets, devices, computer system, or networks, whether physical or virtual so vital to the United Republic of Tanzania that their incapacitation affect national security or the economy and social well being of citizens.

Offences relating to critical information infrastructure

29. Where a person commits an offence under this Act or any written law in relation to critical information infrastructure, that person shall be liable, on conviction to a fine not less than one hundred million shillings or three times the loss occasioned or to imprisonment for a term not less than five years or to both.

PART III
JURISDICTION

Jurisdiction

30.-(1) The courts shall have jurisdiction to try any offence under this Act where an act or omission constituting an offence is committed wholly or in part -

(a) within the United Republic of Tanzania;

(b) on a ship or aircraft registered in the United Republic of Tanzania;

(c) by a national of the United Republic of Tanzania;

(d) by a national of the United Republic of Tanzania who resides outside the United Republic of Tanzania, if the act or omission would equally constitute an offence under a law of that country; or

(e) by any person, irrespective of his nationality or citizenship, or location, when the offence is:

(i) committed using a computer system, device or data located within United Republic of Tanzania; or

(ii) directed against computer system, device or data or person located in United Republic of Tanzania.

(2) In this section the term "court" means court of competent jurisdiction.

PART IV
SEARCH AND SEIZURE

Search and seizure

31.-(1) Police officer incharge of a police station or a law enforcement officer of a similar rank, upon being satisfied that there are reasonable grounds to suspect or believe that a computer system-

(a) may be used as evidence in proving an offence; or

(b) is acquired by any person as a result of an offence,

issue an order authorizing a law enforcement officer to:

(i) enter into any premise and search or seize a device or computer system;

(ii) secure the computer data accessed; or

(iii) extend the search or similar accessing to another system where a law enforcement officer conducting a search has grounds to believe that the data sought is stored in another computer system or part of it.

(2) The search under this section shall be conducted in accordance with the relevant laws regulating the conduct of search and seizure.

(3) Where a device or computer system is removed

or rendered inaccessible following a search or a seizure, the law enforcement officer shall, at the time of the search or as soon as practicable after the search-

(a) prepare a list of items seized or rendered inaccessibleand time of seizure; and

(b) issue a copy of that list to the person having control of the computer system.

(4) A person having custody or control of the computer system may request from a law enforcement officer a permission to access or copy computer data on the system after seizure.

(5) Without prejudice to subsection (4), the law enforcement officer may refuse to give access or provide a copy the information if he has reasonable grounds to believe that giving the access or providing the copy-

(a) would constitute an offence; or

(b) would prejudice -

(i) investigation in connection with the search;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that are pending or that may be instituted in relation to any investigation.

(6) In this section "premise" includes land, buildings, vessel or aircraft.

Disclosure of data

32.-(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, a police officer in charge of a police station or a law enforcement officer of a similar rank may issue an order to any person in possession of such data compelling him to disclose such data

(2) The order issued under subsection (1) shall be granted to a law enforcement officer who shall serve the order to the person in possession of the data.

(3) Where the disclosure of data cannot be done under subsection (1), the law enforcement officer may apply to the court for an order compelling:

(a) a person to submit specified data that is in that person's possession or control; or

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

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

Expedited preservation

33.-(1) Where there is a reasonable ground to believe that a computer data that is required for the purpose of investigation is vulnerable to loss or modification, the police officer incharge of a police station or a law enforcement officer of a similar rank may issue an order requiring the person in control of a device or computer data to preserve the device or computer data for a period not exceeding fourteen days.

(2) The court may, on application, extend the order made under section 35 for such period as the court may deem necessary.

Disclosure and collection of traffic data

34.-(1) where there is a reasonable ground that a computer data is required for the purpose of investigation, a police officer in charge of a police station or a law enforcement officer of a similar rank may issue an order to any person in possession of the data for-

(a)disclosure, collection or recording of the traffic data associated with a specified communication during a specified period; or

(b) permitting and assisting the law enforcement officer to collect or record that data.

(2) For the purposes of this section, "traffic data" means-

(a) information relating to communication by means of a computer system;

(b) the information generated by computer system that is part of the chain of communication; and

(c) information that shows the communication's origin, destination, route, time, size, duration or the type of underlying service.

Disclosure and collection of content data

35. where there is a reasonable ground to suspect or believe that the content of an electronic communication is required for the purposes of investigation, a police officer incharge of a police station or a law enforcement officer of a similar rank may issue an order -

(a) to collect, record, permit or assist the relevant authority to collect or record content data associated with specified communications transmitted by means of a computer system; or

(b) to collect or record the computer data through technical means.

Court order

36. Where the disclosure or preservation of data, under sections 31, 32, 33, 34 and 35, as the case may be,

can not be done without the use of force or due to resistance from the part holding data or evidential value of data can be preserved through the order of the court, a law enforcement officer may apply to court for an order for the disclosure or preservation.

Use of forensic tool

37.-(1) Where a law enforcement officer is satisfied that essential evidence cannot be collected under this Part, he may apply to the court for an order to authorise the use of a forensic tool.

(2) The application under subsection (1) shall contain-

(a) the name and address of the suspect;

(b) a description of the targeted computer system; and

(c) a description of the intended measures, purpose, extent and duration of the utilization.

(3) The law enforcement officer 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 law enforcement officer shall log-

(a) the technical means used and 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 fourteen days.

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

(8) Where the installation process requires a site visit, the requirements of section 30 shall apply.

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

(10) The Minister may, by notice published in the *Gazette* prescribe offences under which the court may grant an order for utilization of a forensic tool.

Hearing of application

38. The proceedings for hearing of an application under this part shall be *exparte* and in camera.

PART V
LIABILITY OF SERVICE PROVIDERS

Monitoring obligation

39.-(1) When providing services in accordance with the provisions of this Part, a service provider shall not -

(a) monitor the data which the service provider transmit or store; or

(b) actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may prescribe procedures for service providers to-

(a) inform the competent authority of alleged illegal activities undertaken or information provided by recipients of their service; and

(b) avail competent authorities, at their request, with

information enabling the identification of recipients of their service.

(3) A service provider shall not be liable for disclosure, by a third party, of data lawfully made available to the third party upon proving that-

(a) the third party acted without the knowledge of the service provider; or

(b) the service provider exercised due care and skill to prevent the disclosure of such data.

(4) Where a service provider has knowledge of illegal information, or activity he shall -

(a) remove the information in the computer system within the service providers control;

(b) suspend or terminate services in respect of that information or activity; and

(c) notify appropriate law enforcement authority of the illegal activity or information, relevant facts and the identity of the person for whom the service provider is supplying services in respect of the information.

Access Provider

40.-(1) An access provider shall not be liable for providing access, transmitting or operating computer system in respect of third-party material in the form of electronic communication to which he merely provides access to or for operating facilities via a computer system under his control, provided that he-

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; or

(c) does not select or modify the information contained in the transmission.

(2) The transmission and provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place-

(a) for the purpose of carrying out the transmission in the information system;

(b) in a manner that makes it inaccessible to a person other than the anticipated recipient; and

(c) for a period no longer than is reasonably necessary for the transmission.

Hosting provider

41.-(1) A hosting provider is not liable for information stored at the request of a user of the service, on condition that the hosting provider -

(a) immediately removes or disables access to the information after receiving an order from any competent authority or court to remove specific illegal information stored; or

(b) upon becoming aware of illegal information stored in means than a competent authority, shall immediately inform the relevant authority.

(2) The provision of subsection (1) shall not apply where the user of the service is acting under the authority or control of the hosting provider.

Caching provider

42. A caching provider shall not be liable for the storage of information provided that the caching provider:

(a) does not modify the information;

(b) complies with conditions of access to the information;

(c) complies with rules regarding the updating of the information;

(d) does not interfere with the lawful use of the technology widely recognised and used in the industry, to obtain data on the use of the information; and

(e) acts immediately to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or the relevant authority has ordered such removal or disablement.

Hyperlink provider

43. A hyperlink provider is not liable for the information linked provided that the hyperlink provider :

(a) immediately removes or disables access to the information after receiving an order to do so from the relevant authority; and

(b) upon becoming aware of the specific illegal information stored by other ways than an order from a public authority, immediately informs relevant authority.

Search engine provider

44.-(1) A search engine provider is not liable for search results, on condition that the search engine provider-

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission.

(2) For the purpose of this section, a search engine provider is a person who makes or operates a search engine whtih creates an index of Internet related content or makes available electronic tools to such for information provided by third party.

Take-down Notification

45.-(1) A person may, through a take-down notification, notify the service provider of-

(a) any data or activity infringing the rights of the recipient or of a third party;

(b) any unlawful material or activity; or

(c) any other matter conducted or provided contrary to the provisions of any written law

(2) For purposes of this part, a takedown notification shall be in a permanent medium addressed by the complainant to the service provider or its designated agent and shall include-

(a) the full names and address of the complainant;

(b) the signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of unlawful activity;

(e) the remedial action required to be taken by

the service provider in respect of the complaint;

(f) a statement that the complainant is acting in good faith; and

(g) a statement by the complainant that the information in the take-down notification is to his knowledge true or correct

(3) A person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts commits an offence and is liable, on conviction, to a fine not less than five million or to imprisonment of a term not less than one year or both.

(4) A service provider who fails to take action on the take-down notification received under this section, shall be charged as a person who initiated the contents of subsection (1).

(5) Any person who communicates a take-down notification to a service provider and the service provider fails to act upon the notification, the person may notify a competent authority of the failure to take-down and the competent authority may take down or order the service provider to act on the take down notification or take any other measures to resolve the matter.

(6) A service provider shall not be liable for a take-down done in compliance to a notification under this Act.

Other obligations not affected

46. This Part shall not affect obligation of a service provider that-

(a) has been formed by an agreement;

(b) is acting as such under a licensing or other regulatory regime established under any written law;

(c) has been imposed by law or by order of a court to remove, block or deny access to any

electronic communication or to terminate or prevent unlawful activity.

PART VI
GENERAL PROVISIONS

Immunity

47.-(1) Notwithstanding any other law to the contrary, anything done by law enforcement officer in the execution of functions conferred upon such law enforcement officer under this Act, render such law enforcement officer personally liable for such matter or thing.

(2) A person shall not be liable in respect of the performance of any act or omission where such act or omission was done in good faith and without negligence in accordance with the provisions of this Act.

Forfeiture of property

48.-(1) In addition to a penalty imposed under this Act, the court may order forfeiture of any-

(a) property constituting traceable proceeds of such offence; and

(b) device or property used or intended to be used to commit or to facilitate the commission of the offence.

(2) In addition to an order that may be made under subsection (1), the court may order the convicted person to pay the victim of the offence such compensation as the Court may deem just.

Offence by corporate body

49. If a corporate body is convicted of an offence under this Act, every person who, at the time of commission of the offence was -

(a) a director, officer or is otherwise concerned with

the management of, the corporate body; or

(b) knowingly authorised or permitted the act or omission constituting the offence,

is deemed to have committed the same offence unless every such person proves that the commission of the offence took place without his consent or that he exercised due diligence to prevent the commission of offence and may be proceeded against and punished accordingly.

Compounding of offences

50.-(1) Without prejudice to any other law in force in Mainland Tanzania, the Director of Public Prosecutions may, at any time prior to the commencement of court proceedings and subject to a voluntary admission of the commission of offence under this Act compound the offence and order that person to pay a sum of money specified by him but not exceeding the amount of fine prescribed for any of such offence.

(2) The compounding order under subsection (1) shall be-

(a) in writing, specifying the offence committed, the sum of money to be paid and the date for payment and have attached the written admission referred to in sub-section (1);

(b) final and not subject to any appeal; and

(c) enforced in the same manner as an order of the High Court.

Powers to make regulations

51. The Minister may make regulations with respect to any matter which, by this Act, is required to be prescribed or which is necessary for giving effect to this Act.

PART VII
CONSEQUENTIAL AMENDMENTS

(a) Amendment of the Electronic and Postal Communications Act, 2010

Construction No.3 of 2010

52. This Part shall be read as one with the Electronic and Postal Communications Act, hereinafter referred to as the "principal Act".

Amendment of Section 124

53. The principal Act is amended in section 124, by –

(a) deleting the marginal note and substituting for it the following "Establishment of the National Computer Emergency Response Team"

(b) deleting sub-section 3.

(b) Amendment of the Penal Code, Cap.16

Construction Cap. 16

54. This Part shall be read as one with the Penal Code, hereinafter referred to as the "principal Act".

Amendment of Section 109

55. The principal Act is amended in section 109, by:

(a) designating sectin 109 as section 109(1);

(b) inserting the word "device" immediately after the word "document" that appears in subsection (1) as renamed.

(c) Amendment of the Anti-Money Laundering Act, Cap.423

Construction Cap.423

56. This Part shall be read as one with the Anti-Money Laundering Act, hereinafter referred to as the principal Act.

Amendment of section 3

57. The principal Act is amended in section 3, by -

(a) inserting a new paragraph (r) immediately after paragraph (q) appearing in the definition of the term "predicate offence" as follows:

"(r) offences under Cyber Crimes Act, 2015" and

(b) renaming paragraphs (r) to (y) as paragraphs (s) to (z).

(d) Amendment of the Extradition Act, Cap.368

Construction Cap.368

58. This Part may be cited as the Extradition Act, and shall be read as one with the Extradition Act, hereinafter referred to as the principal Act.

Amendment of the Schedule

59. The principal Act is amended in the Schedule by adding immediately after the heading "slave dealings" the following:

"Cybercrimes

Offences under the Cybercrimes Act, 2015."

Passed in the National Assembly on the 1st April, 2015.

.....

Clerk of the National Assembly