UNDERSTAND THE TANZANIA CYBERCRIMES ACT 2015

SIMPLIFIED LANGUAGE

ENGLISH VERSION

Prepared by:
Samson Mmari
Chairman
FOLEA
Mwanza,Tanzania
Tell:+255766324781
Email: muammarsamson@yahoo.com

Forum for Legal Assistance-FOLEA
Mwanza,Tanzania
Tell:+255766324781
Email: legal.assistance01@yahoo.com

Tanzania Cybercrimes Act, 2015 it was tabled before the National Parliament of the United Republic of Tanzania as a bill on March 2015 by the Ministry of Communication Science and Technology during the 19th National Assembly meeting under the emergence certificate..

This book contains a simplified language which will create awareness to the readers on the objectives and purposes of the Tanzania Cybercrimes Act,2015.Reader will understands offences related to computer systems and information communication technologies that have criminalized, investigation, collection and the use of electronic evidence as provided by the Act,

This book is a reflection of part II, III, IV, V, VI of the Tanzania Cybercrimes Act, 2015.Part II provides for the provisions relating to offences committed and relative penalties, part III deals with the jurisdiction of courts in relation to the offences committed, part IV provides for procedures and powers of search and seizure of the properties suspected to have been used in the commission of offence, part V contains provisions that relate to liability of service providers for the purpose of prescribing the extent and manner in which service providers are liable during provision of online services, part VI provides for general provisions which include, immunity to law enforcement officers when executing their duties, forfeiture of properties, provisions relating to offences committed by corporate body, powers of the Director of Public Prosecutions to compound offences and powers of the Minister to make Regulations.

"OUR life today depends on information technology (InfoTech). From communication, transport, finance and banking, to energy and education, the importance of InfoTech cannot be overemphasized"

CHAPTER 1
PROVISIONS RELATING TO OFFENCES AND PENALTIES

Illegal access
A person shall not intentionally and unlawfully access or cause a computer system to be accessed; A person who goes against 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 imprisonment for a term of not less than one year or to both.

Illegal remaining
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/she was allowed to access the computer system. A person who 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
A person shall not intentionally and unlawfully; intercept by technical means or by any other means a non-public transmission to, from or within a computer system, a non-public electromagnetic emission from a computer system and a non-public computer system that is connected to another computer system; or circumvent the protection measures implemented to prevent access to the content of non-public transmission.
A person who go against 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

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 either by mutilating, removing or modifying the data, program or any other form of information existing within or outside a computer system, 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 creating, altering, or destroying a password, personal identification number, code or method used to access it, such person 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.

A person who communicates, discloses or transmits any computer data, program, access code or command to an unauthorized person; receives unauthorized 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.

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-

i. Mutilating, removing or modifying the data, program or any other form of information existing within or outside a computer system;
ii. 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

iii. Creating, altering, or destroying a password, personal identification number, code or method used to access a computer system,

Such person 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

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

A person who go against 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

A person who unlawfully hinders or interferes with the functioning of a computer system or 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

A person shall not unlawfully deal with or possess a device, including a computer program, that is designed or adapted for the purpose of committing an offence, 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.

A person who goes against 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 fraud

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 for legal purposes as if it were authentic, regardless of whether or not the data is readable or intelligible.

A person who goes against 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

A person shall not cause a loss of property to another person by any input, alteration, deletion, delaying transmission or suppression of computer data or any interference with the functioning of a computer system, with fraudulent or dishonest intent.

A person who goes against 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
A person shall not publish child pornography, through a computer system or make available or facilitate the access of child pornography through a computer system.

A person who goes against 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 imprisonment for a term of not less than seven years or to both.

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
A person shall not publish or cause to be published through a computer system or through any other information and communication technology pornography or pornography which is lascivious or obscene.

A person who goes against commits an offence and is liable on conviction, in the case of publication of 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 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
A person shall not, by using a computer system impersonate another person. A person who goes against 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
Any person who publishes information, data or facts presented in a picture, text, symbol or any other form in a computer system where such information, data or fact is false, deceptive, misleading or inaccurate commits an offence, and shall on conviction be liable to a fine not less than three million shillings or to imprisonment for a term not less than six months or to both.

Racist and Xenophobic material
A person shall not, through a computer system; produce racist or xenophobic material for the purposes of distribution, offer or make available racist or xenophobic material or distribute or transmit racist or xenophobic material.

A person who goes against 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
A person shall not insult another person through a computer system on the basis of race, colour, descent, nationality, ethnic origin or religion.
A person who insult another person through a computer system on the basis of race, colour, descent, nationality, ethnic origin or religion 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
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.
A person who goes against 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.

Unsolicited messages
A person shall not initiate the transmission of unsolicited messages, relay or retransmit unsolicited messages, or falsify header information in unsolicited messages.

A person who goes against 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.
Unsolicited messages mean any electronic message which is not solicited by the recipient.

Disclosure of details of investigation
A person shall not disclose details of a criminal investigation, which requires confidentiality. A person who discloses details of a criminal investigation, which requires confidentiality 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
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.

A person who intentionally and unlawfully prevents the execution or fails to comply with an order issued under the Tanzania Cybercrimes Act, 2015 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
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.

A person who goes against 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.

Violation of Intellectual property rights
A person shall not use a computer system to violate intellectual property rights protected under any written law.

A person who use a computer system to violate intellectual property rights protected commits an offence and in case the infringement is on 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
If the infringement is on commercial basis, a said person 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.

Principal offenders
Any person who does an act or makes an omission which constitutes an offence, does or omits to do any act for the purpose of enabling or aiding another person to commit an offence, aids or abets another person in committing an offence;

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.

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

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.

It is immaterial except so far as regards to punishment, whether the offender does all that is necessary on his part for completing the commission of the offence or the complete fulfilment of his intention is prevented by circumstances independent of his will; or he desists of his own motion from further execution of his intention.

That by reason of circumstances not known to the offender it is impossible to commit the offence.

A person who attempts to commit an offence under the Tanzania Cybercrimes Act, 2015 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
Any person who conspires with another person to commit an offence under the Tanzania Cybercrimes Act,2015, 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
The Minister may, by order published in the *Gazette*, designate a computer system as critical information infrastructure. The order may prescribe guidelines or procedures in respect of-

i. Registration, protection or preservation of critical information Infrastructure.
ii. General management of critical information infrastructure.
iii. Access to, transfer and control of data in any critical information infrastructure.
iv. Integrity and authenticity of data or information contained in any critical information infrastructure.
v. Methods to be used in the storage or archiving data or information in critical information infrastructure.
vi. Disaster recovery plans in the event of loss of the critical information infrastructure or any part of critical information infrastructure.
vii. Manner and procedure for carrying out audit and inspection on any critical information infrastructure; and

Any other matter that is relevant for adequate protection, management and control of data and other resources in a critical information infrastructure.

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
Where a person commits an offence under the Tanzania Cybercrimes Act,2015 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.

JURISDICTION

Jurisdiction
The courts shall have jurisdiction to try any offence under the Tanzania Cybercrimes Act, 2015 where an act or omission constituting an offence is committed wholly or in part:

i. Within the United Republic of Tanzania;
ii. On a ship or aircraft registered in the United Republic of Tanzania;
iii. By a national of the United Republic of Tanzania;
iv. 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
v. By any person, irrespective of his nationality or citizenship, or location, when the offence is:
    a. Committed using a computer system, device or data located within United Republic of Tanzania; or
    b. Directed against computer system, device or data or person located in United Republic of Tanzania.

According to the Tanzania Cybercrimes Act, 2015 court means any court of competent jurisdiction.

SEARCH AND SEIZURE

Search and seizure
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:

i. May be used as evidence in proving an offence; or
ii. Is acquired by any person as a result of an offence,
iii. issue an order authorizing a law enforcement officer to:
    a. Enter into any premise and search or seize a device or computer system;
    b. Secure the computer data accessed; or
    c. 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.

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

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.

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.

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:

i. Would constitute an offence; or
ii. Would prejudice :
    a. Investigation in connection with the search;
    b. Another ongoing investigation; or

c. Any criminal proceedings that are pending or that may be instituted in relation to any investigation.

According to the Tanzania Cybercrimes Act,2015 Premise includes land, buildings, vessel or aircraft.

Disclosure of data

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

The order issued shall be granted to a law enforcement officer who shall serve the order to the person in possession of the data.

Where the disclosure of data can not be done as provided by this law the law enforcement officer may apply to the court for an order compelling:

i. A person to submit specified data that is in that person's possession or control; or
ii. A service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.

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

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.

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

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:

i. Disclosure, collection or recording of the traffic data associated with a specified communication during a specified period; or
ii. Permitting and assisting the law enforcement officer to collect or record that data.

According to the Tanzania Cybercrimes Act,2015 traffic data means:

i. Information relating to communication by means of a computer system;
ii. The information generated by computer system that is part of the chain of communication; and
iii. Information that shows the communication's origin, destination, route, time, size, duration or the type of underlying service.

Disclosure and collection of content data

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 :

i. 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
ii. To collect or record the computer data through technical means.

Court order

Where the disclosure or preservation of data, under sections 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

Where a law enforcement officer is satisfied that essential evidence cannot be collected he may apply to the court for an order to authorise the use of a forensic tool.

The application to the court for an order to authorize the use of a forensic tool shall contain:

i. The name and address of the suspect;
ii. A description of the targeted computer system; and
iii. A description of the intended measures, purpose, extent and duration of the utilization.

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.

During investigation, the law enforcement officer shall log:

i. The technical means used and time and date of the application;
ii. The identification of the computer system and details of the

modification undertaken within the investigation;

iii. Any information obtained;

The information obtained under during investigation shall be protected against any modification, unauthorized deletion and unauthorized access. The authorization shall be valid for a period of fourteen days.

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

Where the installation process requires a site visit, the requirements of section 30 of the Tanzania Cybercrimes Act, 2015 shall apply.

In addition to the order granted the order to authorize the use of a forensic tool, the court may, on application, order the service provider to support the installation process of the forensic tool.

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

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

LIABILITY OF SERVICE PROVIDERS

No monitoring obligation

When providing services in accordance with the provisions of Part five of the Tanzania Cybercrimes Act, 2015, a service provider shall not:

i. Be obliged to monitor the data which the service provider transmit or store; or

ii. Actively seek facts or circumstances indicating an unlawful activity.

The Minister may prescribe procedures for service providers to:

i. Inform the competent authority of alleged illegal activities undertaken or information provided by recipients of their service; and
ii. To avail competent authorities, at their request, with information enabling the identification of recipients of their service.

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:

i. The third party acted without the knowledge of the service provider; or
ii. The service provider exercised due care and skill to prevent the disclosure of such data.

Where a service provider has actual knowledge of illegal information, or activity he shall:

i. Remove the information in the computer system within the service providers control;
ii. Suspend or terminate services in respect of that information or activity; and
iii. 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

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:

i. Does not initiate the transmission;
ii. Does not select the receiver of the transmission; or
iii. Does not select or modify the information contained in the transmission.

The transmission and provision of access referred; include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place:

i. For the purpose of carrying out the transmission in the information system;
ii. In a manner that makes it inaccessible to a person other than the anticipated recipient; and
iii. For a period no longer than is reasonably necessary for the transmission.

Hosting provider

A hosting provider is not liable for information stored at the request of a user of the service, on condition that the hosting provider:

i. 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
ii. Upon becoming aware of illegal information stored in means than a competent authority, shall immediately inform the relevant authority.

NOTE: The above paragraph shall not apply where the user of the service is acting under the authority or control of the hosting provider.

Caching provider

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

i. Does not modify the information
ii. Complies with conditions of access to the information;
iii. Complies with rules regarding the updating of the information;
iv. 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
v. 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

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

i. Immediately removes or disables access to the information after receiving an order to do so from the relevant authority; and
ii. 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

A search engine provider is not liable for search results, on condition that the search engine provider:

i. Does not initiate the transmission;
ii. Does not select the receiver of the transmission; and
iii. Does not select or modify the information contained in the

transmission.

A search engine provider is a person who makes or operates a search engine which creates an index of Internet related content or makes available electronic tools to such for information provided by third party.

Take-down Notification

A person may, through a take-down notification, notify the service provider of:

i. Any data or activity infringing the rights of the recipient or of a thirdparty;
ii. Any unlawful material or activity; or
iii. Any other matter conducted or provided contrary to the provisions of any written law

A takedown notification shall be in a permanent medium addressed by the complainant to the service provider or its designated agent and shall include:

i. The full names and address of the complainant;
ii. The signature of the complainant;
iii. Identification of the right that has allegedly been infringed
iv. Identification of the material or activity that is claimed to be the subject of unlawful activity;
v. The remedial action required to be taken by the service provider in respect of the complaint;
vi. A statement that the complainant is acting in good faith;
vii. A statement by the complainant that the information in the take-down notification is to his knowledge true or correct

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.

A service provider shall not be liable for a take-down done in compliance to a notification under the Tanzania Cybercrimes Act, 2015.

Otherobligations notaffected

Part five of the Tanzania Cybercrimes Act,2015 shall not affect obligation of a service provider that:

i. Has been formed by an agreement
ii. Is acting as such under a licensing or other regulatory regime established under any written law
iii. 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.

GENERAL PROVISIONS

Immunity

Anything done by law enforcement officer in the execution of functions conferred upon such law enforcement officer under the Tanzania Cybercrimes Act,2015 render such law enforcement officer personally liable for such matter or thing.

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 the Tanzania Cybercrimes Act, 2015.

Forfeiture of property

In addition to a penalty imposed under the Tanzania Cybercrimes Act,2015 the court may order forfeiture of any:

i. Property constituting traceable proceeds of such offence; and
ii. Device or property used or intended to be used to commit or to facilitate the commission of the offence.

In addition to an order forfeiture that may be made, the court

may order the convicted person to pay the victim of the offence such compensation as the Court may deem just.

A person convicted of an offence under the Tanzania Cybercrimes Act, 2015 shall surrender travelling document to the relevant authority until that person pays the fine or served the sentence imposed on him.

Offence by corporate body

If a corporate body is convicted of an offence under the Tanzania Cybercrimes Act,2015 every person who, at the time of commission of the offence was:

i. A director, officer or is otherwise concerned with the management of, the corporate body; or
ii. 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

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 the Tanzania Cybercrimes Act,2015 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.

The compounding order under shall be:

i. 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 above.
ii. Final and not subject to any appeal; and
iii. Enforced in the same manner as an order of the High Court.

Powers to make regulations

The Minister may make regulations with respect to any matter which, by The Tanzania Cybercrimes Act,2015 is required to be prescribed or which is necessary for giving effect to the Act.