

THE UNITED REPUBLIC OF TANZANIA  
***BILL SUPPLEMENT***

***No. 4***

***20<sup>th</sup> February, 2015***

*to the Gazette of the United Republic of Tanzania No.8 Vol.96 dated 20<sup>th</sup> February, 2015*  
*Printed by the Government Printer, Dar es Salaam by Order of Government*

---

**THE CYBERCRIMES ACT, 2015**

ARRANGEMENT OF SECTIONS

*Section*

*Title*

PART I  
PRELIMINARY PROVISIONS

1. Short Title and commencement.
2. Application.
3. Interpretation.

PART II  
PROVISIONS RELATING TO OFFENCES AND PENALTIES

4. Illegal Access.
5. Illegal remaining.
6. Illegal interception.
7. Illegal data interference.
8. Data espionage.
9. Illegal system interference.
10. Illegal device.
11. Computer-related forgery.
12. Computer-related fraud.

13. Child pornography.
14. Pornography.
15. Identity related crimes.
16. Publication of false information.
17. Racist and xenophobic material.
18. Racist and xenophobic motivated insult.
19. Genocide and crimes against humanity.
20. Unsolicited messages.
21. Disclosure of details of an investigation.
22. Obstruction of investigation.
23. Cyber bullying.
24. Violation of intellectual property rights.
25. Principal offenders.
26. Attempt.
27. Conspiracy to commit offence.
28. Protection of critical information infrastructure.
29. Offences relating to critical information infrastructure.

PART III  
JURISDICTION

30. Jurisdiction.

PART IV  
SEARCH AND SEIZURE

31. Search and Seizure.
32. Disclosure of data.
33. Expedited preservation.
34. Disclosure and collection of traffic data.
35. Disclosure and collection of content data.
36. Court order.
37. Use of forensic tool.
38. Hearing of application.

PART V  
LIABILITY OF SERVICE PROVIDERS

- 39. No monitoring obligation.
- 40. Access provider.
- 41. Hosting provider.
- 42. Caching provider.
- 43. Hyperlink provider.
- 44. Search engine provider.
- 45. Take-down notification.
- 46. Other obligations not affected.

PART VI  
GENERAL PROVISIONS

- 47. Immunity.
- 48. Forfeiture of property.
- 49. Offences by corporate body.
- 50. Compounding of offences.
- 51. Powers to make regulations.

PART VII  
CONSEQUENTIAL AMENDMENTS

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

- 52. Construction.
- 53. Amendment of section 124.

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

- 54. Construction.

55. Amendment of section 109.

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

56. Construction

57. Amendment of section 3.

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

58. Construction

59. Amendment of the Schedule.

**NOTICE**

This Bill to be submitted to the National Assembly is published for general information to the public together with a statement of its objects and reasons.

Dar es Salaam,  
3<sup>rd</sup> February, 2015

**OMBENI Y. SEFUE**  
*Secretary to the Cabinet*

**A BILL**  
*for*

**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 | <b>1.</b> 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 <i>Gazette</i> appoint.                                 |
| Application                  | <b>2.</b> Save for section 50, this Act shall apply to Mainland Tanzania as well as Tanzania Zanzibar.  |
| Interpretation               | <b>3.</b> In this Act, unless the context otherwise requires –<br>“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 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.** 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) 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 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-

**11.**-(1) A person shall not intentionally and unlawfully input, alter, delay

related forgery 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.

(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, 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

**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.

Unsolicited messages

**20.**-(1) A person shall not -

- (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 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 three million shillings or to imprisonment for a term of not less than one year or to both.

Violation of  
intellectual  
property rights

**24.**-(1) A person shall not use a computer system 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.

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 months 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 inaccessible and 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 can not 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 *ex parte* and in camera.

#### PART V LIABILITY OF SERVICE PROVIDERS

No monitoring obligation

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

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

provider 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 which 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 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.

(3) A person convicted of an offence under this Act 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

**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 section 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.”

---

**OBJECTS AND REASONS**

The Bill proposes the enactment of a law which will make provisions for criminalizing offences related to computer systems and Information Communication Technologies; to provide for investigation, collection, and use of electronic evidence.

The proposed law is divided into Seven Parts.

Part I provides for preliminary provisions relating to the short title and commencement, provisions for application, and interpretation of terms used in the proposed law.

Part II provides for the provisions relating to offences committed and relative penalties under the proposed law.

Part III deals with the jurisdiction of courts in relation to the offences committed under the proposed law.

Part IV provides for procedures and powers of search and seizure of the properties suspected to have been used in the commission of offence under the proposed law.

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.

Lastly, Part VII provides for the consequential amendments to various laws for the purposes of harmonizing proposed law with the existing laws.

Dar es Salaam,  
2 Februari, 2015

**MAKAME M. MBARAWA**  
*Minister of Communication Science  
and Technology*

SHERIA YA MAKOSA YA MTANDAO, 2015

MPANGILIO WA VIFUNGU

*Kifungu*      *Kichwa cha habari*

SEHEMU YA KWANZA  
MASHARTI YA AWALI

1. Jina na tarehe ya kuanza kutumika.
2. Matumizi.
3. Tafsiri.

SEHEMU YA PILI  
MASHARTI YANAYOHUSIANA NA MAKOSA NA ADHABU

4. Kuingia kinyume cha sheria.
5. Kubaki katika mfumo wa kompyuta kinyume cha sheria.
6. Kuingilia mawasiliano kinyume cha sheria.
7. Kuingilia data kinyume cha sheria.
8. Ujasusi data.
9. Kuingilia mfumo kinyume cha sheria.
10. Kifaa kisicho halali.
11. Kughushi kunakohusiana na masuala ya kompyuta.
12. Udanganyifu unaohusiana na kompyuta.
13. Ponografia za watoto.
14. Ponografia.
15. Makosa yanayohusiana na utambuzi.
16. Kutoa taarifa za uongo.
17. Ubaguzi.
18. Matusi ya kibaguzi.
19. Mauaji ya kimbari.
20. Taarifa zinazotumwa bila ridhaa.
21. Kufichua taarifa za upelelezi.
22. Kuzuia upelelezi.

23. Unyanyasaji kwa kupitia mtandao.
24. Ukiukaji wa haki bunifu.
25. Wakosaji wakuu.
26. Jaribio la kufanya uhalifu.
27. Kula njama ya kutenda kosa.
28. Ulinzi wa miundo mbinu muhimu ya TEHAMA.
29. Uhujumu wa miundo mbinu muhimu ya TEHAMA.

SEHEMU YA TATU  
MAMLAKA YA MAHAKAMA

30. Mamlaka ya mahakama.

SEHEMU YA NNE  
UPEKUZI NA UKAMATAJI

31. Upekuzi na ukamataji.
32. Utoaji data.
33. Utunzaji data wa dharura.
34. Utoaji na ukusanyaji wa mwenendo wa data.
35. Utoaji na ukusanyaji wa maudhui katika data.
36. Amri ya mahakama.
37. Matumizi ya kifaa cha TEHAMA katika uchunguzi.
38. Usikilizaji wa maombi.

SEHEMU YA TANO  
WAJIBU WA WATOA HUDUMA

39. Kutowajibika kufanya ufuatiliaji.
40. Mtoa huduma ya kuingia kwenye mfumo.
41. Mtunza data.
42. Mhifadhi data kwa muda mfupi.
43. Mtoa huduma ya kuunganisha tovuti.
44. Mtoa huduma ya utafutaji wa taarifa.
45. Notisi ya kuondoa.
46. Wajibu mwingine kutoathiriwa na sheria.

SEHEMU YA SITA  
MASHARTI YA JUMLA

47. Kinga.
48. Utaifishaji mali.
49. Makosa yanayofanywa na kampuni.
50. Kufifilisha kosa.
51. Mamlaka ya kutengeneza kanuni.

**TAARIFA**

Muswada huu utakaowasilishwa Bungeni umechapishwa pamoja na madhumuni na sababu zake kwa ajili ya kutoa taarifa ya jumla kwa umma.

Dar es Salaam,  
3 Februari, 2015

**OMBENI Y. SEFUE**  
*Katibu wa Baraza la Mawaziri*

**MUSWADA**  
*wa*

**Sheria inayoainisha makosa yanayohusiana na matumizi ya mfumo wa kompyuta na Teknolojia ya Habari na Mawasiliano, kuweka utaratibu wa upelelezi, ukusanyaji na matumizi ya ushahidi wa kielektroniki na masuala mengine yanayohusiana na hayo.**

**IMETUNGWA** na Bunge la Jamhuri ya Muungano wa Tanzania.

**SEHEMU YA KWANZA**  
**MASHARTI YA AWALI**

Jina na tarehe  
ya kuanza  
kutumika

**1.** Sheria hii itaitwa Sheria ya Makosa ya Mtandao ya mwaka 2015. Sheria hii itaanza kutumika tarehe ambayo Waziri ataiteua na kuitangaza katika *Gazeti la Serikali*.

Matumizi

**2.** Isipokuwa kwa kifungu cha 50, Sheria hii itatumika Tanzania Bara na Tanzania Zanzibar.

Tafsiri

**3.** Katika sheria hii, isipokuwa kama muktadha utahitaji vinginevyo-  
“kuingia” kuhusiana na mfumo wa kompyuta maana yake ni kuingia, kutoa maelekezo, kuwasiliana, kuhifadhi data au kupokea data kutoka katika mfumo wa kompyuta au vinginevyo kutumia rasilimali zozote za mfumo wa kompyuta au



- mtandao au chombo cha kuhifadhi data;
- “mtoa njia” maana yake ni mtu anayetoa huduma ya usambazaji wa data za kielektroniki kwa kusambaza taarifa zilizotolewa na au kwa mtumiaji wa huduma katika mtandao wa mawasiliano au anayetoa fursa ya kuingia kwenye kompyuta au mtandao;
- “mhifadhi data ” maana yake ni mtu anayetoa huduma ya uhifadhi wa data za kielektroniki kwa njia inayojiendesha yenyewe, kwa kupitia mtu kati au kwa utunzaji wa taarifa kwa muda mfupi kwa madhumuni ya kuwezesha upatikanaji wa taarifa kwa kwa watumiaji wengine wa huduma kiufanisi zaidi pale watakapoomba;
- “mtoto” maana yake ni mtu mwenye umri chini ya miaka kumi na nane;
- “ponografia za watoto” maana yake ni aina yoyote ya picha na filamu za ngono zinazo ashiria au kumuonesha:
- (a) mtoto akiwa anashiriki kwa uwazi katika matendo ya ngono;
  - (b) mtu anayeonekana kama mtoto akiwa anashiriki kwa uwazi katika matendo ya ngono; au
  - (c) taswira inayoashiria mtoto akiwa anashiriki kwa udhahiri katika matendo ya ngono;
- “mfumo wa kompyuta” maana yake ni kifaa au mchanganyiko wa vifaa, ikijumuisha mtandao, vifaa vya kuingizia na vya kutolea na ambavyo vinaweza kutumika pamoja na majalada yaliyo na programu za kompyuta, maelezo ya kielektroniki, data za kuingizia na data za kutolea zinazotunza data za hesabu za miongo zilizo na mantiki na udhibiti wa utolewaji wa mawasiliano na majukumu mengine;
- “data kompyuta” maana yake ni uwasilishaji wa maelezo, dhana, taarifa au maelekezo katika namna inayofaa kwa ajili ya kuchakata katika mfumo wa kompyuta, ikijumuisha programu inayofaa kwa ajili ya kuwezesha mfumo wa kompyuta kutelekeza kazi fulani;
- “chombo cha utunzaji wa data ” maana yake ni kifaa chochote au kitu ambacho kutoka kwake data kompyuta au taarifa inaweza kuchakata kwenye mfumo wa kompyuta au kutengenezwa ama kwa msaada wa kifaa kingine au kitu au la;
- “kifaa” inajumuisha:
- (a) programu ya kompyuta, namba tambuzi, mianzi laini au *application*;

(b) sehemu ya mfumo wa kompyuta kama vile grafiki kadi, kadi ya kutunza kumbukumbu, chipu au kichakataji;

(c) kifaa cha kutunzia kumbukumbu za kompyuta; na

(d) kifaa cha kuingizia na kutolea taarifa katika kompyuta na mifumo ya kompyuta;

“mawasiliano ya kielektroniki” maana yake ni uhamishaji wa alama, ishara au data kompyuta ya aina yoyote ile iliyotumwa yote au sehemu kwa njia ya waya, redio, elektromagnetiki, picha ya kielektroniki, picha ya mfumo wa optika au aina nyingine ya mfumo inayofanana na hiyo;

“ kifaa cha TEHAMA katika uchunguzi ” maana yake ni kifaa cha uchunguzi au kifaa kinachojumuisha mianzi laini au mianzi ngumu iliyowekwa kwenye au inayohusiana na mfumo wa kompyuta au sehemu ya mfumo wa kompyuta na inayotumika kutekeleza kazi zinazojumuisha uingiaji kwa siri au ukusanyaji wa taarifa za kiuchunguzi zinazohusiana na matumizi ya kompyuta au mfumo wa kompyuta;

“zuia” kuhusiana na mfumo wa kompyuta inajumuisha-

(a) kusababisha kuingiliwa kielektromagnetiki kwa mfumo wa kompyuta;

(b) kuvuruga mfumo wa kompyuta kwa namna yoyote ile; au

(c) kuingiza, kutuma, kuzorotesha, kufuta, kuvuruga, kubadilisha au kuzuia data kompyuta;

“mtunza data” maana yake ni mtu anayetoa huduma ya kusambaza data kwa kutunza taarifa inayotolewa na mtumiaji wa huduma hiyo;

“kiunganishi tovuti” maana yake ni alama, neno, msemu, sentensi, au taswira iliyo katika tovuti au taarifa kuhusiana na chanzo kingine kinachopelekea au kufunguka kwa tovuti nyingine;

“haki bunifu” maana yake ni haki zinazotokana au zinazohusiana na haki miliki, hati bunifu, alama za biashara, na mambo mengine yanayohusiana nayo;

“kuingilia” kuhusiana na utendaji kazi wa kompyuta inajumuisha upatikanaji, utazamaji, usikilizaji au kunukuu data yoyote ya mawasiliano ya kompyuta au mifumo ya kompyuta kwa njia yoyote ya kielektroniki;

“afisa utekelezaji wa sheria” maana yake ni afisa wa polisi mwenye cheo cha Mkaguzi Msaidizi wa Polisi, mpelelezi, afisa Usalama wa Taifa mwendesha mashtaka au mtu aliyeidhinishwa chini ya sheria yoyote;

“Waziri” maana yake ni Waziri anayehusika na masuala ya TEHAMA.

“kuchapisha” maana yake ni usambazaji, uwasilishaji, uwekaji wazi, kubadilishana, uchapishaji, au usambazaji wa aina yoyote ile;

“mali” maana yake ni mali ya aina yoyote, inayogusika au isiyo gusika na inajumusha:

- (a) fedha yoyote inayotumika au isiyotumika katika Jamhuri ya Muungano Tanzania;
- (b) taarifa, ikijumuisha programu, data au nakala zake, zinazoweza kusomwa na binadamu au kwa kompyuta; au
- (c) haki yoyote au maslahi kwenye mali;

“ubaguzi” maana yake ni taarifa za namna yoyote zinazokuza au kuchochea chuki, ubaguzi au vurugu dhidi ya mtu au kundi la watu kwa msingi wa tabaka, rangi, asili, utaifa, kabila au dini;

“mtoa huduma” maana yeke ni mtu au upande unaowezesha mfumo wa taarifa kupatikana kwa mtu-kati.

#### SEHEMU YA PILI

#### MASHARTI YANAYOHUSIANA NA MAKOSA NA ADHABU

Kuingia  
kinyume cha  
sheria

**4.**-(1) Mtu hataingia au kusababisha kuingiliwa mfumo wa kompyuta kinyume cha sheria na kwa makusudi.

(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni tatu au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungu kwa kipindi kisichopungua mwaka mmoja au vyote.

Matumizi ya  
mfumo wa  
kompyuta  
kinyume cha

**5.**-(1) Mtu hatatumia au kuendelea kutumia mfumo wa kompyuta, kinyume cha sheria na kwa makusudi, baada ya kuisha kwa muda ambao aliruhusiwa kutumia mfumo wa kompyuta.

sheria

(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni moja au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua miezi sita au vyote.

Kuingilia mawasiliano kinyume cha sheria

**6.-(1)** Mtu ambaye, kinyume cha sheria na kwa makusudi-

(a) anaingilia kwa kutumia njia ya kiufundi au kwa njia nyingine yoyote:

- (i) mawasiliano yasiyo ya umma kwenda au kutoka au yaliyo ndani ya mfumo wa kompyuta;
- (ii) mawasiliano yasiyo ya umma ya kielektronaniginetiki yakokayo katika mfumo wa kompyuta usio wa umma; au
- (iii) mfumo wa kompyuta usio wa umma ambao umeunganishwa na mfumo mwingine wa kompyuta.

(b) anakwepa hatua za udhibiti zilizoelekezwa kwa ajili ya kukinga kuingiliwa kwa maudhui yaliyomo kwenye mawasiliano yasiyo ya umma.

(2) Mtu atakayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini isiyo pungua shilingi milioni tano au kutumikia kifungo kwa kipindi kisichopungua mwaka mmoja au vyote.

Kuingilia data kinyume cha sheria

**7.-(1)** Mtu ambaye, kinyume cha sheria na kwa makusudi-

(a) anaharibu au anazorotesha data kompyuta;

(b) anafuta data kompyuta;

(c) anabadili data kompyuta;

(d) anaifanya datamkompyuta ipoteze maana, ishindwe kutumika au ikose ufanisi;

(e) anazuia au anaingilia matumizi halali ya data kompyuta;

(f) anazuia au anamuingilia mtu mwingine anayetumia data kompyuta kihalali; au

(g) anamzuia mtu aliyeidhinishwa kutumia data kompyuta, atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni kumi au mara tatu ya thamani ya faida iliyopatikana kinyume na sheria au kutumikia kifungo kwa kipindi kisichopungua miaka mitatu au vyote.

(2) Mtu ambaye-

(a) anawasilisha, anafichua au anasambaza data kompyuta, programu ya kompyuta, ishara ya kuingilia au agizwa kwa mtu ambaye hajaidhinishwa;

(b) anapokea data kompyuta ambayo hajaidhinishwa, ametenda kosa na akitiwa hatiani, atawajibika, kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni mbili au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua mwaka mmoja au vyote.

(3) Mtu ambaye isivyo halali na kwa makusudi anaharibu au anabadili data yoyote ya kompyuta, iwapo data hiyo inatakiwa kutunzwa kisheria au ni ushahidi kwenye shauri lolote chini ya Sheria hii kwa-

(a) kuondoa au kubadilisha data, programu au taarifa nyingine yoyote iliyoko ndani au nje ya mfumo wa kompyuta;

(b) anawasha, anaingiza au anapakua programu ambayo imetengenezwa kwa lengo la kuondoa au kubadilisha data, programu au aina yoyote ya taarifa iliyoko ndani au nje ya mfumo wa kompyuta; au

(c) anatengeneza, anabadilisha au anaharibu namba ya siri, namba binafsi ya utambulisho au namna inayotumika kuingika kwenye mfumo wa kompyuta, atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni ishirini au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua miaka mitano au vyote.

Ujasusi data  
Sura ya 47

**8.**-(1) Bila kuathiri masharti ya sheria ya Usalama wa Taifa, mtu hataingilia pasipo idhini na kujipatia data kompyuta iliyokingwa dhidi ya kuingiliwa.

(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni ishirini au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua miaka mitano au vyote

Kuingilia  
mfumo  
kinyume cha  
sheria

**9.** Mtu ambaye, kinyume cha sheria na kwa makusudi anazuia au anaingilia-

(a) utendaji kazi wa mfumo wa kompyuta;

(b) matumizi au uendeshaji wa mfumo wa kompyuta, atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho

ni kikubwa kati ya kiwango kisichopungua shilingi milioni mbili au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua mwaka mmoja au vyote

Kifaa kisicho halali

**10.-(1)** Mtu hatajishughulisha au kumiliki, kinyume cha sheria-

- (a) kifaa ikijumuisha programu ya kompyuta iliyotengenezwa au inayotumiwa kwa madhumuni ya kutenda kosa;
- (b) namba ya siri ya kompyuta, ishara ya kuingilia au data kama hiyo ambayo inaweza kutumika na mtu yoyote kuingilia mfumo wa kompyuta au sehemu yake kwa lengo la kutenda kosa.

(2) Mtu akatayekiuka kifungo kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika, kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni kumi au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua miaka mitatu au vyote

Kughushi kunakohusiana na masuala ya kompyuta

**11.-(1)** Mtu hataingiza, hatabadilisha, hatachelewesha, hatasambaza au hatafuta data kompyuta iliyogushiwa kwa lengo la kutaka itumike kwa madhumuni halali, bila kujali kama taarifa hiyo inasomeka au haisomeki.

(2) Mtu akatayekiuka kifungo kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika, kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni ishirini au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua miaka saba au vyote.

Udanganyifu unaohusiana na kompyuta

**12.-(1)** Mtu hatasababisha kupotea kwa mali ya mtu mwingine-

- (a) kwa kuongeza, kubadilisha, kufuta, kuchelewesha, kusambaza au kuzuia data kompyuta; au
- (b) kwa kuingilia utendaji kazi wa mfumo wa kompyuta, kwa udanganyifu au ya uongo kwa lengo la kujipatia bila haki manufaa ya kiuchumi.

(2) Mtu akatayekiuka kifungo kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika, kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni ishirini au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua

miaka saba au vyote.

Ponografia za watoto

**13.-(1) Mtu yeyote-**

- (a) hatachapisha ponografia za watoto kwa kupitia mfumo wa kompyuta; au
- (b) hatawezesha upatikanaji au kuoneshwa kwa ponografia za mtoto kwa kupitia mfumo wa kompyuta.

(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni hamsini au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungu kwa kipindi kisichopungua miaka saba au vyote.

(3) Mtu aliyetiwa hatiani kwa kosa chini ya kifungu hiki, pamoja na adhabu nyingine yoyote, anaweza kuamriwa kumlipa fidia mtu ambaye ameathirika na kosa hilo.

Ponografia

**14.-(1) Mtu hatachapisha au kusababisha kuchapishwa kwa kupitia katika mfumo wa kompyuta-**

- (a) ponografia; au
- (b) ponografia yoyote iliyo ya kiasherati au chafu.

(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika, iwapo ni uchapishaji kuhusiana na-

- (a) ponografia, kulipa faini isiyopungua shilingi milioni ishirini au kutumikia kifungu kwa kipindi kisichopungua miaka saba au vyote; au
- (b) ponografia iliyo ya kiasherati au chafu, kulipa faini isiyopungua shilingi milioni thelathini au kutumikia kifungu kwa kipindi kisichopungua miaka kumi au vyote.

Makosa yanayohusiana na utambuzi

**15.-(1) Mtu hatajifanya kuwa mtu mwingine kwa kutumia mfumo wa kompyuta.**

(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni tano au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungu kwa kipindi kisichopungua miaka saba au vyote.

Kutoa taarifa za

**16. Mtu yeyote anayetoa taarifa, data au maelezo kwa njia ya picha,**

- uongo maandishi, alama au aina nyingine yoyote kwenye mfumo wa kompyuta, endapo taarifa, data, au maelezo hayo ni ya uongo, yanapotosha au yasiyo sahihi, atakuwa ametenda kosa, na akipatikana na hatia atalipa faini isiyopungua shilingi milioni tatu au kutumikia adhabu ya kifungo kisichopungua miezi sita au vyote.
- Ubaguzi **17.**-(1) Mtu, kwa kutumia mfumo wa kompyuta-  
(a) hatazalisha vitu vya kibaguzi kwa madhumuni ya kuvisambaza;  
(b) hatatoa au kuwezesha kupatikana vitu vya kibaguzi ; au  
(c) hatarusha vitu vya kibaguzi.  
(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini isiyopungua kiasi cha shilingi milioni tatu au kutumikia kifungo kwa kipindi kisichopungua mwaka mmoja au vyote.
- Matusi ya kibaguzi **18.**-(1) Mtu hatamdhihaki mtu mwingine kwa kupitia mfumo wa kompyuta, kutokana na sababu kuwa mtu huyo mwingine ni mmoja kati ya kundi linalotambulika kwa tabaka, rangi, asili, utaifa, kabila au dini fulani.  
(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini isiyopungua shilingi milioni tatu au kutumikia kifungo kwa kipindi kisichopungua mwaka mmoja au vyote.
- Mauaji ya kimbari **19.**-(1) Mtu hatachapisha au kusababisha kuchapishwa vitu vinavyochochea, kanusha, punguza au halalisha matendo yanayopelekea mauaji ya kimbari na makosa dhidi ya binadamu kwa kupitia mfumo wa kompyuta.  
(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini isiyopungua shilingi milioni kumi au kutumikia kifungo kwa kipindi cha kisichopungua miaka mitatu au vyote.
- Taarifa zinazotumwa bila ridhaa **20.**-(1) Mtu-  
(a) hataanzisha usambazaji wa taarifa zinazotumwa bila ridhaa;  
(b) hatarusha tena au kusambaza upya taarifa zinazotumwa bila ridhaa;  
(c) hataghushi taarifa za utambulisho na kuzituma bila ridhaa  
(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika kulipa faini ya kiasi ambacho ni kikubwa kati ya kiwango kisichopungua shilingi milioni tatu au mara tatu ya thamani ya faida iliyopatikana kinyume cha sheria, au kutumikia kifungo kwa kipindi kisichopungua mwaka mmoja



au vyote.

(3) Kwa madhumuni ya kifungu hiki, “taarifa zinazotumwa bila ridhaa” maana yake ni taarifa au data za kielektroniki amabazo hazijaombwa na mpokeaji.

Kufichua  
taarifa za  
upelelezi

**21.**-(1) Mtoa huduma anayepokea amri kuhusiana na upelelezi wa kijinai, inayohitaji usiri, hatatoa taarifa yoyote iliyopo kwenye amri hiyo isivyo halali na makusudi.

(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na atawajibika, iwapo atatiwa hatiani, kulipa faini isiyopungua shilingi milioni kumi au kutumikia kifungu kwa kipindi kisichopungua miaka mitatu au vyote.

Kuzuia  
upelelezi

**22.** Mtu ambaye kwa makusudi na kinyume cha sheria ataharibu, atafuta, ataondoa, ataficha, atabadilisha au ataifanya data kompyuta kukosa maana kwa lengo la kuharibu ushahidi au kuchelewesha upelelezi atakuwa ametenda kosa na akitiwa hatiani atawajibika kulipa faini ya kiwango kisichopungua milioni tatu au kutumikia kifungu kwa muda usiopungua mwaka mmoja au vyote.

(2) Mtu ambaye kwa makusudi atazuia utekeleza au atashindwa kutekeleza amri iliyotolewa na sheria hii, atakuwa ametenda kosa na atawajibika, iwapo atatiwa hatiani, kulipa faini isiyopungua shilingi milioni tatu au kutumikia kifungu kwa kipindi cha kisichopungua mwaka mmoja au vyote.

Unyanyasaji  
kwa kupitia  
mtandao

**23.**-(1) Mtu hataanzisha au kukadimisha mawasiliano yoyote ya kielektroniki kwenda kwa mtu yoyote kwa kutumia mfumo wa kompyuta, kwa lengo la kurubuni, kulazimisha, kutisha au kunyanyasa au kusababisha maudhi ya hisia.

(2) Mtu akataye kiuka kifungu kidogo cha (1) atakuwa ametenda kosa na atawajibika, iwapo atatiwa hatiani, kulipa faini isiyopungua shilingi milioni tatu au kutumikia kifungu kwa kipindi cha kisichopungua mwaka mmoja au vyote.

Ukiukaji wa  
haki bunifu

**24.**-(1) Mtu hatatumia mfumo wa kompyuta kwa lengo la kukiuka haki bunifu zinazolindwa na Sheria nyingine yoyote.

(2) Mtu akatayekiuka kifungu kidogo cha (1) atakuwa ametenda kosa na akitiwa hatiani, atawajibika iwapo ukiukaji -

(a) hauhusiani na masuala ya kibiashara, kulipa faini isiyo pungua shilingi milioni tano au kutumikia kifungu kwa kipindi kisichopungua miaka mitatu au vyote;

(b) unagusa masuala ya kibiashara, kulipa faini isiyo pungua shilingi milioni

ishirini au kutumikia kifungo kwa kipindi kisichopungua miaka mitano au vyote.

Wakosaji  
wakuu

**25.**-(1) Mtu yeyote ambaye-

- (a) anafanya kitendo au anaacha kufanya kitendo ambacho kiasi kwamba kutokutenda huko kunasababisha kutendeka kwa kosa;
- (b) anafanya au anaacha kufanya kitendo kwa madhumuni ya kumuwezesha au kumsaidia mtu mwingine kutenda kosa;
- (c) anamsaidia na kumuwezesha mtu mwingine kutenda kosa;
- (d) anamshawishi au kumlipa mtu mwingine kufanya kosa hilo, atachukuliwa kuwa ametenda kosa na atashitakiwa kama mtu aliyetenda kosa.

(2) Mtu anayemlipa mtu mwingine kufanya au kutokufanya kitendo kwa kiasi ambapo, iwapo yeye mwenyewe angefanya kitendo hicho au kutokutenda huko, kitendo hicho kingepelekea kosa kufanyika kwa upande wake na atakuwa na hatia kwa kosa la aina hiyo na atawajibika kwa adhabu sawa kana kwamba yeye mwenyewe angefanya kitendo hicho au kutokutenda huko.

Jaribio la  
kufanya uhalifu

**26.**-(1) Pale ambapo mtu anayekusudia kutenda kosa anaanza kutekeleza kusudio lake na anadhihirisha kusudio lake kwa kitendo kinachoashiria kosa, isipokuwa hatekelezi kusudio lake kwa kiasi cha kutenda kosa hilo, atachukuliwa kuwa ametenda kosa hilo.

(2) Kwa madhumuni ya kifungu hiki-

(a) isipokuwa kwa kiasi cha adhabu haitajalisha iwapo-

- (i) mkosaji anatenda yote ambayo ni muhimu kwa utendaji wa kosa; au
- (ii) utekelezaji wa kusudio lake kwa ukamilifu unazuiliwa na mazingira ambayo hayaingiliani na kusudio lake; au
- (iii) anaacha kutekeleza kusudio lake kwa hiari yake mwenyewe;

(b) kutokana na sababu za mazingira yasiyojulikana kwa mhalifu haiwezekani kutenda kosa.

(3) Mtu yeyote anayejaribu kutenda kosa chini ya sheria hii atakua ametenda kosa na akitiwa hatiani atawajibika kulipa faini isiyopungua shilingi milioni moja au kifungo kwa kipindi kisichopungua miezi sita au vyote.

Kula njama ya  
kutenda kosa

**27.** Mtu anayekula njama na mtu mwingine kutenda kosa chini ya Sheria hii, anatenda kosa na iwapo atatiwa hatiani, atawajibika kulipa faini isiyopungua shilingi

milioni moja au kutumikia kifungo kwa kipindi kisichopungua mwaka mmoja au vyote.

Ulinzi wa  
miundo mbinu  
muhimu ya  
TEHAMA

**28.**-(1) Waziri anaweza, kwa amri itakayochapishwa kwenye *Gazeti la Serikali* kuainisha mifumo ya kompyuta kama miundombinu muhimu.

(2) Amri iliyorejewa chini ya kifungo kidogo cha (1) inaweza kuainisha vigezo, miongozo na taratibu kuhusiana na-

- (a) usajili, ulinzi au utunzaji;
- (b) usimamizi wa jumla;
- (c) kuingia, kuhamisha na kudhibiti data;
- (d) kuhakikisha uwepo wa audilifu au uhalali wa data au taarifa;
- (e) njia zitakazotumika kuhifadhi au kutunza data;
- (f) mipango ya kudhibiti majanga iwapo kutatokea uharibifu;
- (g) namna na utaratibu wa kuendesha ukaguzi;
- (h) jambo jingine lolote ambalo ni muhimu kwa ulinzi, usimamizi na udhibiti wa data na rasimali nyingine.

(3) Kwa madhumuni ya kifungu hiki, miundombinu muhimu ya TEHAMA inajumuisha mali, vifaa, mifumo ya kompyuta au mitandao inayoshikika na isiyoshikika ambayo ina umuhimu kwa Jamhuri ya Muungano wa Tanzania kiasi kwamba kutokufanya kazi kwake kuna madhara ya kiusalama, kiuchumi na kijamii.

Uhujumu wa  
miundombinu  
muhimu wa  
TEHAMA

**29.** Pale ambapo mtu anatenda kosa chini ya sheria hii au sheria nyingine yoyote linalohusiana na miundombinu muhimu, mtu huyo atakuwa ametenda kosa na akitiwa hatiani atawajibika kulipa faini isiyopungua shilingi milioni mia moja au mara tatu ya hasara aliyoisababisha au kifungo kisichopungua miaka mitano au vyote.

#### SEHEMU YA TATU MAMLAKA YA MAHAKAMA

Mamlaka ya  
mahakama

**30.**-(1) Mahakama zitakuwa na uwezo wa kusikiliza shauri lolote chini ya Sheria hii pale ambapo kosa au sehemu ya kosa -

- (a) limetendeka ndani ya Jamhuri ya Muungano wa Tanzania;
- (b) limetendeka kwenye meli au ndege iliyosajiliwa ndani ya Jamhuri ya Muungano wa Tanzania;
- (c) limetendwa na mtanzania; au
- (d) limetendwa na mtanzania anayeishi nje Jamhuri ya Muungano wa Tanzania,

- endapo kitendo alichokitenda mtu huyo kingekuwa ni kosa chini ya sheria ya nchi hiyo;
- (e) limetendwa na mtu yeyote, bila kujali utaifa au ukaazi wake au eneo husika, iwapo kosa limefanyika-
- (i) kwa kutumia mfumo wa kompyuta, kifaa au data zilizoko ndani ya Jamhuri ya Muungano wa Tanzania; au
  - (ii) dhidi ya mfumo wa kompyuta, kifaa au data au mtu aliye ndani ya Jamhuri ya Muungano wa Tanzania.
- (2) Katika kifungu hiki, neno “mahakama” lina maana ya mahakama yenye mamlaka.

SEHEMU YA NNE  
UPEKUZI NA UKAMATAJI

Upekuzi na  
ukamataji

- 31.**-(1) Askari Polisi mkuu wa kituo au afisa utekelezaji wa sheria mwenye cheo cha askari mkuu wa kituo, baada ya kuridhika kuwa kuna sababu za msingi kushuku au kuamini kuwa mfumo wa kompyuta-
- (a) unaweza kutumika kuthibitisha kosa;
  - (b) unachukuliwa na mtu yeyote kutokana na kosa,
- kutoa hati ya upekuzi itakayo muidhinisha afisa utekelezaji wa sheria -
- (i) kuingia kwenye eneo kwa lengo la kupekua au kukamata kifaa au mfumo wa kompyuta;
  - (ii) kuiwekea ulinzi data iliyopatikana;
  - (iii) kuongeza wigo wa upekuzi au uwezo wa kuingia kwenye mfumo mwingine iwapo afisa utekelezaji wa sheria anayefanya upekuzi anazo sababu za kuaminika kuwa data inayotafutwa, inatunzwa kwenye mfumo mwingine wa kompyuta au sehemu yake.
- (2) Upekuzi chini ya kifungu hiki utafanyika kwa mujibu wa sheria zinazo simamia masuala ya upekuzi na ukamataji wa mali.
- (3) Iwapo kifaa au mfumo wa kompyuta umeondolewa au hauingiliki kutokana na upekuzi au ukamataji wa mali, afisa utekelezaji wa sheria, wakati wa upekuzi na ukamataji wa mali -
- (a) ataandaa orodha ya vitu vyote vilivyokamatwa au kufanywa visiingilike, ikijumuisha muda ambao mali ilikamatwa;
  - (b) atampatia nakala ya orodha ya mali iliyokamatwa mtu anayemiliki au mwangalizi wa mfumo husika wa kompyuta.

(4) Mtu anayemiliki au mwangalizi wa mfumo wa kompyuta anaweza kumuomba afisa utekelezaji wa sheria ruhusa ya kuingia au kudurufu taarifa zilizopo kwenye mfumo wa kompyuta baada ya ukamataji wa mali.

(5) Bila kuathiri masharti ya kifungu kidogo cha (4), afisa utekelezaji wa sheria anaweza kukataa kuruhusu kuingia kwenye mfumo au kudurufu taarifa iwapo anazo sababu za msingi za kuamini kuwa kuruhusu kuingia au kudurufu taarifa-

(a) itakuwa ni kosa; au

(b) kutaathiri-

(i) uchunguzi unaohusiana na upekuzi

(ii) upelelezi mwingine unaoendelea; au

(iii) shauri lolote lililopo mahakamani au ambalo linaweza kufunguliwa kuhusiana na uchunguzi huo.

(6) Katika kifungu hiki “eneo” inajumuisha ardhi, majengo au chombo cha usafiri.

Utoaji data

**32.**-(1) Pale ambapo data inanitajika kuwekwa wazi kwa madhumuni ya uchunguzi wa kijinai au kuendeshwa kwa kesi mahakamani, Askari Polisi Mkuu wa kituo au afisa mtekelezaji wa sheria mwenye cheo cha askari mkuu wa kituo anaweza kutoa amri kumtaka-

(a) mtu yeyote kuwasilisha data iliyoainishwa ambayo mtu huyo anaimiliki au iliyo chini ya uangalizi wake ambayo imehifadhiwa kwenye mfumo wa kompyuta; au

(b) mtoa huduma yeyote, kuwasilisha taarifa kuhusiana na mteja zilizo kwenye umiliki au uangalizi wake.

(2) Iwapo kitu chochote kinachohusiana na upelelezi kinajumuisha data iliyohifadhiwa kwenye mfumo wa kompyuta au kwenye kifaa, amri itachukuliwa kumtaka mtu kutoa au kuruhusu upatikanaji wa data hiyo katika namna ambayo inasomeka na inayoweza kuondolewa.

Utunzaji data  
wa dharura

**33.** Pale ambapo Askari Polisi Mkuu wa kituo au afisa utekelezaji wa sheria anazo sababu za kuamini kuwa data kompyuta ambayo inahitajika kwa madhumuni ya uchunguzi inaweza kupotea au kubadilishwa, anaweza kutoa amri itakayomtaka mtu mwenye uangalizi au umiliki wa kifaa au data kompyuta kuitunza kwa kipindi kisichozidi siku kumi na nne.

Utoaji na

---

**34.**-(1) Pale Askari Polisi Mkuu wa kituo au afisa mtekelezaji wa sheria

ukusanyaji wa data nyendo

mwenye cheo cha askari mkuu wa kituo anaridhika kuwa data kompyuta inahitajika kwa madhumuni ya uchunguzi, afisa huyo anaweza kutoa amri kwa maandishi kwa ajili ya-

- (a) ukusanyaji au kuweka kumbukumbu za taarifa za kompyuta zinazohusiana na mawasiliano maalum kwa kipindi maalum; au
- (b) kumruhusu na kumsaidia afisa utekelezaji wa sheria kukusanya na kuweka kumbukumbu za data hizo.
- (2) Kwa madhumuni ya kifungu hiki “data nyendo” maana yake ni taarifa:
  - (a) inayohusiana na mawasiliano kwa mfumo wa kompyuta;
  - (b) iliyotolewa na mfumo wa kompyuta ambao ni sehemu ya mlolongo wa mawasiliano; na
  - (c) inayoonesha chanzo cha mawasiliano, njia iliyotumika, muda, ukubwa, uelekeo na aina ya huduma zinazoambatana nazo.

Utoaji na ukusanyaji wa maudhui katika data

**35.** Pale ambapo Askari Polisi Mkuu wa kituo au afisa mtekelezaji wa sheria mwenye cheo cha askari mkuu wa kituo anazo sababu za msingi za kushuku au kuamini kuwa yaliyomo kwenye mawasiliano ya kielektroniki yanahitajika kwa madhumuni ya uchunguzi, anaweza kutoa amri ya:

- (a) kukusanya, kurekodi, kuruhusu au kuisaidia mamlaka husika kukusanya au kurekodi taarifa zilizomo kwenye inayohusishwa na mawasiliano maalum yaliyotolewa ka njia ya mfumo wa kompyuta; au
- (b) kumuidhinisha afisa utekelezaji wa sheria kukusanya au kurekodi data kwa kupitia njia ya kiufundi.

Amri ya mahakama

**36.** Pale ambapo utoaji data au utunzaji data wa dharura chini ya vifungu vya 31, 32, 33, 34 au 35 kwa kadri itakavyokuwa, hauwezi kufanyika bila kutumia nguvu au kutokana na pingamizi kutoka kwa mtu mwenye kumiliki data au thamani ya ushahidi katika data inaweza kuhifadhiwa kwa amri ya mahakama, afisa mtekelezaji wa sheria anaweza kuomba mahakamani amri ya utoaji au utunzaji wa data.

Matumizi ya kifaa cha TEHAMA katika uchunguzi

**37.**-(1) Pale ambapo afisa utekelezaji wa sheria anaridhika kuwa ushahidi wa msingi hauwezi kukusanywa kwa kutumia utaratibu uliainishwa chini ya Sehemu hii, afisa utekelezaji huyo anaweza kuiomba mahakama kutoa amri ya kuidhinisha matumizi ya kifaa cha uchunguzi.

- (2) Maombi yaliyotolewa chini ya kifungu kidogo cha (1) yatajumuisha-
  - (a) jina na anuani ya mtuhumiwa;
  - (b) maelezo ya mfumo wa kompyuta unaolengwa; na

- (c) maelezo ya hatua zinazokusudiwa kuchukuliwa, madhumuni, kiasi na muda wa matumizi unaokusudiwa.
- (3) Afisa utekelezaji wa sheria atahakikisha kuwa mabadiliko yaliyofanywa kwenye mfumo wa kompyuta au data iliyomo kwenye kompyuta kuhusiana na mtuhumiwa zinajikita kwenye marekebisho yaliyo ya msingi kwa ajili ya uchunguzi na kwamba mabadiliko yanafanywa baada ya kukamilika kwa uchunguzi.
- (4) Wakati wa uchunguzi, afisa utekelezaji wa sheria ataingiza:
- (a) mbinu za kiufundi zilizotuimika, muda na terehe ya maombi;
- (b) utambuzi wa mfumo wa kompyuta na maelezo ya mabadiliko yaliyofanyika wakati wa uchunguzi;
- (c) taarifa yoyote iliyopatikana;
- (5) Taarifa iliyopatikana italindwa dhidi ya mabadiliko, kufutwa bila ya idhini na kuigia kwenye mfumo bila idhini.
- (6) Idhini iliyotolewa chini ya kifungu kidogo cha (1) itakuwa halali kwa kipindi cha siku kumi na nne.
- (7) Mahakama inaweza, kufuatia maombi, kuongeza muda uliotolewa chini ya kifungu kidogo cha (6) kwa kipindi kingine cha siku kumi na nne au kwa kipindi kingine kwa kadri itakavyoona inafaa.
- (8) Iwapo mchakato wa uwekaji wa kifaa unahitaji kutembelea eneo, masharti ya kifungu cha 30 yatatumika.
- (9) Pamoja na amri iliyotolewa chini ya kifungu kidogo cha (1), mahakama inaweza, kufuatia maombi, kumuamuru mtoa huduma awezeshe mchakato wa kuweka kifaa.
- (10) Waziri anaweza, kwa Taarifa itakayochapishwa kwenye *Gazeti la Serikali*, kuainisha makosa chini ya Sheria hii ambayo mahakama inaweza kutoa amri ya kutumia kifaa cha TEHAMA katika uchunguzi.

Usikilizaji wa maombi

**38.** Utaratibu wa kusikiliza maombi chini ya Sehemu hii utafanywa kwa upande mmoja na kwa siri.

#### SEHEMU YA TANO WAJIBU WA MTOA HUDUMA

Kutowajibika kufanya ufuatiliaji

- 39.**-(1) Wakati wa kutoa huduma chini ya Sehemu hii, mtoa huduma-
- (a) hata wajibika kufuatilia data ambayo anaisambaza au kuhifadhi;
- (b) tafuta maelezo au mazingira yanayoashiria shughuli zinazofanywa

kinyume na sheria.

(2) Waziri anaweza kuweka masharti kuhusiana na utaratibu wa watoa huduma kwa jili ya-

(a) kutoa taarifa kwa mamlaka husika ya umma kuhusiana na shughuli zilizo kinyume na sheria zinazofanywa au taarifa inayotolewa na watumiaji wa huduma zao;

(b) kuzipatia mamlaka husika taarifa zitakazoweza kuwatambua watumia huduma, baada ya maombi.

(3) Mtoa huduma hatawajibika kwa uwekaji wazi wa data iliyotolewa kihalali kwa mtu wa tatu baada ya kuthibitisha kwamba:

(a) mtu huyo wa tatu alitenda hivyo pasipo mtoa huduma ya mtandao kufahamu; au

(b) mtoa huduma alitekeleza wajibu unaostahili na alitumia ujuzi ili kuzuia uwekwaji wazi wa data hizo.

(4) Pale ambapo mtoa huduma atakuwa na uelewa juu ya taarifa au kitendo cha kihalifu kwenye mfumo wa kompyuta ambao upo chini ya udhibiti wake, atatakiwa-

(a) kuondoa taarifa juu ya kitendo hicho;

(b) kusimamisha au kusitisha huduma;

(c) kutaarifu mamlaka husika juu ya kitendo au taarifa hiyo, maelezo na utambuzi wa muhusika anayepewa huduma.

Mtoa huduma  
ya kuingia  
kwenye mfumo

**40.**-(1) Mtoa huduma ya uwezo wa kuingia kwenye mfumo hatawajibika kwa kurusha au kuendesha mfumo wa kompyuta kwa ajili ya mtu mwingine ikiwa yeye ni mtoa huduma tu ya kuwezesha kuingia kwenye mfumo wa kompyuta au kuendesha vifaa kupitia mfumo wa kompyuta ulio chini ya mamlaka yake kwa masharti kwamba mtoa huduma:

(a) haanzishi urushaji mawasiliano;

(b) hachagui mpokeaji wa mawasiliano; au

(c) hachagui au habadilishi data iliyoko kwenye mawasiliano.

(2) Mawasiliano na masharti ya uwezo wa kuingia kwenye mfumo wa kompyuta yaliyotolewa chini ya kifungu kidogo cha (1) yatajumuisha, utunzaji wa taarifa iliyosambazwa kwa madhumuni ya kuendeleza mawasiliano kwenye mfumo wa kompyuta kwa njia inayojiendesha yenyewe kwa kupitia mtu kati na kwa muda kwa kuzingatia kwamba mawasiliano yanafanyika kwa-

(a) madhumuni ya kuendesha na kusambaza taarifa katika mfumo wa



- kompyuta;
- (b) namna ambayo kwa kawaida haiwezi kupatikana isipokuwa tu kwa mpokeaji mlengwa;
  - (c) muda ambao sio mrefu sana zaidi ya muda unaofaa kuuwasilisha ujumbe husika kwa mlengwa.

Mtunza Data

- 41.**-(1) Mtunza Data hatawajibika kuhusiana na taarifa zilizohifadhiwa kwa maombi ya mtumiaji wa huduma hiyo, kwa masharti kwamba-
- (a) anaondoa au kusitisha upatikanaji wa taarifa baada ya kupokea amri kutoka taasisi yenye mamlaka au mahakama ya kuondoa taarifa zilizo kinyume cha sheria;
  - (b) baada ya kufahamu kuwa taarifa iliyohifadhiwa iko kinyume cha sheria ataitaarifu mara moja taasisi husika.
- (2) Kifungu kidogo cha (1) hakitatumika pale ambapo mpokeaji anafanya hivyo chini ya mamlaka ya mtoa huduma.

Mhifadhi data  
kwa muda  
mfupi

- 42.** Mtoa huduma ya kuhifadhi data hatawajibika kwa ajili ya utunzaji wa taarifa ikiwa-
- (a) habadilishi taarifa;
  - (b) anatekeleza masharti ya utoaji wa uwezo wa kuingia kwenye mfumo;
  - (c) anatekeleza kanuni kuhusiana na uboreshaji wa taarifa zilizoainishwa katika namna inayotambulika na walio wengi na kutumika kwenye soko;
  - (d) haiingiliani na matumizi halali ya teknolojia inayotambulika na wengi na ianyotumika sokoni kwa ajili ya data kwa ajili ya matumizi ya taarifa hiyo; na
  - (e) anachukua hatua za haraka kuondoa au kusitisha matumizi ya/kufikiwa kwa taarifa ambayo imetunzwa baada ya kupokea taarifa kamili kwamba taarifa iliyo kwenye chanzo cha mawasiliano imeondolewa kutoka kwenye mtandao au ufikiwaji wake umesitishwa/ matumizi yake yamesitishwa au kwamba mahakama au mamlaka husika imeamuru itolewe au isitishwe.

Mtoa huduma  
ya  
kuunganisha  
tovuti

- 43.** Mtoa huduma ya kuunganisha tovuti hatawajibika kwa taarifa aliyounganisha iwapo-
- (a) haraka iwezekanavyo anaondoa au anasitisha matumizi ya taarifa baada ya kupokea amri kutoka kwa mamlaka husika ya kuondoa kuunganishi hicho; na

- (b) baada ya kupata uelewa kuhusiana na taarifa zilizo kinyume na sheria kwa namna nyingine zaidi ya amri ya mamlaka ya umma, haraka iwezekanavyo ataitaarifu mamlaka husika.

Mtoa huduma  
ya utafutaji wa  
taarifa

**44.**-(1) Mtoa huduma ya utafutaji wa taarifa hatawajibika kwa matokeo ya utafutaji huo, kwa masharti kwamba-

- (a) haanzishi mawasiliano;
- (b) hachagui mpokeaji wa mwasiliano; na
- (c) hachagui au kubadilisha taarifa iliyoko kwenye mawasiliano.

(2) Kwa madhumuni ya kifungu hiki, “mtoa huduma ya utafutaji wa taarifa” maana yake ni mtu anayetengeneza au anayeendesha huduma ambayo inatafuta taarifa inayotengeneza kiashiria inayohusiana na taarifa za mtandao au anawezesha upatikanaji wa vifaa vya kielektroniki kwa ajili ya utafutaji wa taarifa inayotolewa na mtu mwingine.

Notisi ya  
kuondoa

**45.**-(1) Mtu anaweza, kupitia notisi ya kuondoa kumtaarifu mtoa huduma-

- (a) kuhusiana na data au taarifa iliyomnyima mpokeaji au mtu wa tatu haki ya huduma;
- (b) vitu au shughuli ambayo ni kinyume cha sheria; au
- (c) suala lolote linalotekelezwa au linalotolewa kinyume cha sheria hii au sheria nyingine.

(2) Kwa madhumuni ya sehemu hii, notisi ya kuondoa itakuwa katika hali ya kudumu ikitumwa na mlalamikaji kwenda kwa mtoa huduma au wakala wake na itajumuisha-

- (a) jina kamili na anuani ya mlalamikaji;
- (b) saina ya mlalamikaji;
- (c) maelezo ya haki inayodaiwa kuvunjwa;
- (d) maelezo juu ya shughuli ambayo inadaiwa kuwa chimbuko la kitendo kilicho kinyume cha sheria;
- (e) hatua ya utatuzi inayotakiwa kuchukuliwa na mtoa huduma kuhusiana na lalamiko;
- (f) maelezo kuwa mlalamikaji anatenda kwa nia njema;
- (g) maelezo ya mlalamikaji kuwa, kwa ufahamu wake, taarifa iliyomo kwenye taarifa zilizochukuliwa ni sahihi.

(3) Mtu anayewasilisha taarifa kwa mtoa huduma kuhusiana na muamala usio

halali, huku akijua kuwa taarifa hiyo ni potofu, atakuwa ametenda kosa na akitiwa hatiani, atatakiwa kulipa faini ya shilingi million tano au kifungo cha mwaka mmoja au vyote.

(4) Mtoa huduma hatawajibika kwa kuondoa taarifa ikiwa ameifanya kwa mujibu wa sheria hii.

Wajibu  
mwingine  
kutoadhiriwa  
na sheria

**46.** Sehemu hii haitaathiri wajibu wa mtoa huduma:

- (a) uliotolewa na makubaliano;
- (b) ambaye anatenda kwa namna hiyo chini ya kibali au mfumo wa usimamizi uliotajwa chini ya sheria yoyote;
- (c) uliotolewa na sheria au amri ya mahakama ili kutoa, kuzuia au kukataza uingiwaji kwenye mawasiliano ya kieletroniki au kusitisha au kuzuia kitendo kisicho cha halali.

SEHEMU YA SITA  
MASHARTI YA JUMLA

Kinga

**47.**-(1) Bila kujali sheria nyingine yoyote kinyume na haya, jambo au kitu chochote kitakachofanywa na afisa utekelezaji wa sheria, katika utekelezaji wa majukumu yake chini ya Sheria hii, hakitampelekea afisa utekelezaji wa sheria kuwajibika moja kwa moja.

(2) Mtu hatawajibika kuhusiana na utekelezaji wa kitendo chochote au kutokutenda, iwapo kitendo hicho au kutokutenda huko kulifanywa kwa nia njema na siyo kwa uzembe, kwa mujibu wa masharti ya Sheria hii.

Utaiwashaji  
mali

**48.**-(1) Pamoja na adhabu iliyotolewa chini ya Sheria hii, mahakama inaweza kutoa amri kwa ajili ya utaiwashaji wa-

- (a) mali yoyote inayoonekana kuwa ni sehemu ya mapato yatokanayo na kosa; na
- (b) chombo chochote au mali iliyotumika au inayokusudiwa kutumika kutenda au kufanikisha utendaji wa kosa.

(2) Pamoja na amri iliyotolewa chini ya kifungu kidogo cha (1), mahakama inaweza kumuamuru mtu aliyetiwa hatiani kumlipa fidia mtu aliyeathirika na kosa hilo kwa kadri ambavyo mahakama itaona inafaa.

(3) Mtu aliyetiwa hatiani kwa kosa lililofanywa chini ya Sheria hii atawasilisha hati yake ya kusafiria kwa mamlaka husika hadi hapo atakapolipa faini

au kutumikia kifungo alichohukumiwa kutumikia.

(4) Bila kujali kifungo kidogo cha (3), mahakama inaweza, kufuatia kuwasilishwa kwa maombi na kwa sababu za msingi, kutoa amri ya kuachiliwa kwa hati za kusafiria za mshitakiwa.

Makosa  
yanayofanywa  
na kampuni

**49.**-(1) Iwapo kampuni inatiwa hatiani kwa kosa chini ya Sheria hii, mtu yeyote ambaye wakati wa utendaji wa kosa-

- (a) alikuwa ni Mkurugenzi, afisa au vinginevyo anahusika na mambo ya utawala wa kampuni hiyo;
- (b) huku akiwa anajua, aliruhusu kitendo kilichopelekea kosa hilo, atachukuliwa kuwa ametenda kosa hilo na anaweza kushitakiwa na kuadhibiwa ipasavyo.

Kufilisha  
kosa

**50.**-(1) Bila kuathiri sheria nyingine inayotumika Tanzania Bara, Mkurugenzi wa Mashtaka, muda wowote kabla ya mwenendo wa mahakama kuanza na kwa kuzingatia tamko la kukiri kosa kwa hiari la mshitakiwa anaweza kufilisha kosa na kuamuru mtu huyo alipe kiasi cha pesa atakachokitaja ambacho hakitazidi kiasi cha faini kwa kosa hilo.

- (2) Amri ya kufilisha kosa chini ya kifungo kidogo cha (1) itakuwa -
  - (a) ya maandishi, ikiainisha kosa lililotendeka, kiasi cha fedha zitakazolipwa na tarehe ya kufanya malipo ikiambatanisha tamko la kukubali kosa lililorejewa chini ya kifungo kidogo cha (1);
  - (b) ni uamuzi wa mwisho na hautakatiwa rufaa; na
  - (c) na uwezo wa kutekelezwa katika namna sawa na amri ya Mahakama Kuu.

Mamlaka ya  
kutengeneza  
Kanuni

**51.** Waziri anaweza kutunga Kanuni kuhusiana na jambo lolote ambalo linatakiwa kuainishwa na Sheria hii au ambalo ni la umuhimu au uharaka kwa ajili ya utekelezaji wa masharti ya Sheria hii.

---

MADHUMUNI NA SABABU

---

Madhumuni ya Muswada huu ni kutunga sheria ambayo itaainisha makosa yanayohusiana na matumizi ya mfumo wa kompyuta na Teknolojia ya Habari na Mawasiliano, kuweka utaratibu wa upelelezi, ukusanyaji na matumizi ya ushahidi wa kielektroniki.

Muswada unaopendekezwa umegawanyika katika Sehemu Saba.

Sehemu ya Kwanza, inaainisha masharti ya awali, ikiwa ni pamoja na jina la Sheria, tarehe ya kuanza kutumika kwa Sheria na tafsiri ya maneno mbalimbali yaliyotumika katika Muswada huu.

Sehemu ya Pili, inaainisha makosa na adhabu dhidi ya makosa hayo ndani ya sheria hii.

Sehemu ya Tatu, inatoa mamlaka ya mahakama katika kusikiliza na kuamua mashauri yanayohusu makosa ya uhalifu wa mtandao yaliyoainishwa katika sheria inayopendekezwa.

Sehemu ya Nne, inaainisha utaratibu juu ya upekuzi na ukamataji wa vifaa vyenye taarifa zinazohitajika kwa ajili ya upelelezi.

Sehemu ya Tano, inaainisha wajibu wa watoa huduma za mtandao wakati wa kutoa huduma hizo.

Sehemu ya Sita, inaweka masharti ya jumla ikiwa ni pamoja na kinga kwa maafisa utekelezaji wa sheria, utafishaji wa mali zinazohusiana na makosa ya mtandao, ufifilishaji wa makosa na uwajibikaji kwa makosa yanayofanywa na kampuni.

Aidha, sehemu hii imeainisha mamlaka ya waziri mwenye dhamana ya kutunga kanuni kuhusiana na masuala yanayohusu utekelezaji wa sheria hii.

Dar es Salaam,  
2 Februari, 2015

**MAKAME M. MBARAWA**  
*Waziri wa Mawasiliano*  
*Sayansi na Teknolojia*