REPUBLIC OF KENYA

TWELFTH PARLIAMENT – SECOND SESSION

THE NATIONAL ASSEMBLY

VOTES AND PROCEEDINGS

THURSDAY, APRIL 26, 2018 (SPECIAL MORNING SITTING)

1. The House assembled at thirty minutes past Nine O'clock

2. The Proceedings were opened with Prayer

3. **Presiding –** the Deputy Speaker

4. **COMMUNICATION FROM THE CHAIR**

The Fourth Chairperson conveyed the following Communication –

"Honourable Members, I wish to report to the House that on 20th April, 2018, the Speaker received notice by the Member for Kibwezi West Constituency, Hon. Dr. Patrick Musimba, MP intending to propose amendments to the Computer and Cybercrimes Bill (National Assembly Bill No. 36 of 2017) at the Committee Stage.

Honourable Members, in his opinion, the Speaker noted that some proposed amendments were substantive and had a Money Bill effect to the extent that they were proposing to create an Institution of cyber security. In this regard, the Speaker directed that –

(a) The proposed amendments be subject to the provisions of Standing Order 131 or that those with Money-Bill effects be moved by the Chairpersons of the relevant Committees and failure to which, the amendments be stayed and not included for consideration;

(b) The proposed amendments that have no Money-Bill effects be carried by the Member for Kibwezi West, subject to harmonizing with those of the Committees.

Honourable Members, I am glad to inform the House that my Office has received information that the amendments were discussed in a forum comprising the Chairpersons of Administration and National Security and the Information, Communication and Innovation and the Mover of amendments, the Hon. Dr. Patrick Musimba, MP. It was agreed that –

(i) The amendments proposing to create an institution of cyber security will be moved by the Chairperson of the Administration and National Security Committee;
(ii) The amendments relating to offences included in the amendments proposed by the Chairperson of Information, Communication and Innovation be moved by that Chairperson; and

(iii) The amendments relating to cybercrime offences and not included in the amendments proposed by the Chairperson of Information, Communication and Innovation be moved separately by the Hon. Dr. Patrick Musimba.

It is for this reason, Hon. Members, that I have allowed the Chairs of Administration and National Security and the Information, Communications and Innovation to move the said amendments and I direct that the Committee of the Whole House on the Bill proceeds as guided. I thank you."

5. PAPERS LAID

The following Papers were laid on the Table –

(a) Estimates of Recurrent and Development Expenditure of the Parliamentary Service Commission for the Year ending 30th June 2019 and Projections for 2019/2020 – 2021;

(b) The Insolvency (General) (Amendment) (No.2) Regulations, 2018 and the Explanatory Memorandum (pursuant to section 730 of the Insolvency Act, 2015); and

(c) Report of the Auditor General on the Financial Statements of the National Constituencies Development Fund of Kathiani Constituency for the year ended 30th June, 2016 and the certificate therein.

(The Leader of the Majority Party)

(d) The Report of the Departmental Committee on Defence and Foreign Relations on the consideration of the African Continental Free Trade Area (AFCFTA) and COMESA-EAC-SADC Tripartite Free Trade Area (TFTA) Agreements.

(Chairperson, Departmental Committee on Defence & Foreign Relations)

(e) The Report of Budget and Appropriations Committee on the Second Supplementary Estimates for the Financial Year 2017/2018.

(Chairperson, Budget and Appropriations Committee)

6. NOTICES OF MOTION

The following Notices were given–

(i) **THAT**, this House adopts the report of the Departmental Committee on Defence and Foreign Relations on the consideration of the African Continental Free Trade Area (AFCFTA) and COMESA-EAC-SADC Tripartite Free Trade Area (TFTA) Agreements, laid on the Table of the House today, Thursday, April 26, 2018 and

pursuant to Section 8 of the Treaty Making and Ratification Act, 2012, **approves** the ratification of the African Continental Free Trade Area (AFCFTA); and, the COMESA-EAC-SADC Tripartite Free Trade Area (TFTA) Agreements.

(Chairperson, Departmental Committee on Defence & Foreign Relations)

(ii) **THAT**, this House adopts the Second Report of the Budget and Appropriations Committee on the Supplementary Estimates for the financial year 2017/2018, laid on the Table of the House today, Thursday, April 26, 2018 and pursuant to the provisions of Articles 233 of the Constitution and Standing Order 243, **approves** the Second Supplementary Estimates for the Financial Year 2017/2018.

(Chairperson, Budget and Appropriations Committee)

7. NOTICE OF MOTION – ADJOURNMENT OF THE HOUSE TO DISCUSS A DEFINITE MATTER OF URGENT NATIONAL IMPORTANCE

Pursuant to provisions of Standing Order 33(1), the Member for Nandi Hills (Hon. Alfred Keter) claimed to move a Motion for adjournment of the House to discuss a definite matter of urgent national importance regarding disasters caused by heavy rains in the country;

And the Deputy Speaker acceding to the claim;

And there being sufficient number of Members rising in their places in support of the claim;

Thereupon, the Deputy Speaker directed that the Motion be moved at 11.30 a.m. today.

8. THE HEALTH LAWS (AMENDMENT) BILL (NATIONAL ASSEMBLY BILL NO.14 OF 2018)

Order for First Reading read;

Bill read a First Time and referred to the relevant Departmental Committee pursuant to Standing Order 127(1)

9. MOTION – REPORT OF THE COMMITTEE ON DELEGATED LEGISLATION ON THE NATIONAL TRANSPORT AND SAFETY AUTHORITY (OPERATION OF COMMERCIAL VEHICLES) REGULATIONS, 2018

Motion made and Question proposed –

THAT, this House adopts the Report of the Committee on Delegated Legislation on its consideration of the National Transport & Safety Authority (Operation of Commercial Vehicles) Regulations, 2018, laid on the Table of the House on Tuesday, April 17, 2018, and pursuant to the provisions of Section 18 of the Statutory Instruments Act, 2013 and Standing Order 210(4)(b) ***annuls in entirety*** the said Regulations.

(Chairperson, Committee on Delegated Legislation – 25.04.2018)

Debate on the Motion having been concluded on Wednesday, April 25, 2018;

Question put and agreed to.

10. COMMITTEE OF THE WHOLE HOUSE

Order for Committee read

IN THE COMMITTEE

The Fourth Chairperson in the Chair

The Computer and Cybercrimes Bill (National Assembly Bill No. 36 of 2017)

Clause 3 - amendment proposed –

THAT, clause 3 of the Bill be amended—

(a) by deleting paragraph (c) and substituting therefor the following new paragraph—

"(c) facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes";

(b) by inserting the following new paragraph immediately after paragraph (c)—

"(ca) protect the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution;"

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to

Clause 3 - as amended agreed to

Clause 4 - agreed to

Clause 5 - amendment proposed –

THAT, clause 5 of the Bill be amended in sub-clause (2) by deleting the word "this" appearing immediately after the words "purposes of";

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to

Clause 5 - as amended agreed to;

Clause 6 - agreed to

Clause 7 - amendment proposed –

THAT, Clause 7 of the Bill be amended in sub-clause (2) by—

(a) inserting the words "or psychological" immediately after the word "physical" appearing in paragraph (c);
(b) deleting the word "of" appearing immediately after the words "for a term" at the end of the sub-clause.

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 7 - as amended agreed to

Clause 8 - amendment proposed –

THAT, clause 8 of the Bill be amended—

(a) in sub-clause (2) by deleting the words "without sufficient excuse or justification" appearing immediately after the words "this Part";

(b) in sub-clause (3) by deleting the words "in thereof" appearing immediately after the word "described" and substituting therefor the words "under the subsections".

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 8 - as amended agreed to

Clause 9 - amendment proposed –

THAT, clause 9 of the Bill be amended in sub-clause (1) by deleting the word "term" appearing immediately after the word "imprisonment".

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 9 - as amended agreed to

Clause 10 - amendment proposed –

THAT, clause 10 of the Bill be amended—

(a) in sub-clause (1) by inserting the words "for a" immediately after the word "imprisonment";

(b) in sub-clause (2)(f) by deleting the words "by the Cabinet Secretary in the manner or form as the Cabinet Secretary may consider appropriate" and substituting therefor the words—

"relating to the security, defence or international relations of Kenya, critical information, communications, business or transport infrastructure and protection of public safety and public services as may be designated by the Cabinet Secretary responsible for matters relating to information, communication and technology."

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to

Clause 10 - as amended agreed to

Clause 11 - amendment proposed –

THAT, clause 11 of the Bill be amended—

(a) by inserting the following new sub-clauses immediately after sub-clause (1)—

"(1A) A person who commits an offence under subsection (1) which causes physical injury to any person is liable, on conviction, to imprisonment for a term not exceeding twenty years.

(1B) A person who commits an offence under subsection (1) which causes the death of a person is liable, on conviction, to imprisonment for life."

(b) in sub-clause (3) by inserting the word "shillings" immediately after the words "five million".

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to

Clause 11 - as amended agreed to

Clause 12 - amendment proposed –

THAT, clause 12 of the Bill be amended by-

(a) renumbering the existing provision as sub-clause (1);

(b) inserting the following new sub-clause immediately after sub-clause (1)-

"(2) Pursuant to Article 24 of the Constitution, the freedom of expression under Article 33 of the Constitution shall be limited in respect of the intentional publication of false, misleading or fictitious data or misinformation that-

(a) is likely to-

(i) propagate war; or

(ii) incite persons to violence;

(b) constitutes hate speech;

(c) advocates hatred that-

(i) constitutes ethnic incitement, vilification of others or incitement to cause harm; or

(ii) is based on any ground of discrimination specified or contemplated in Article 27(4) of the Constitution; or

(d) negatively affects the rights or reputations of others.

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to

Clause 12 - as amended agreed to

Clause 13 - amendment proposed –

THAT, clause 13 of the Bill be deleted;

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Proposed amendment withdrawn;

Further amendment proposed -

THAT, clause 13 of the Bill be amended—

(a) in sub clause (1)-

(i) by inserting the following new paragraph (ba) immediately after paragraph (b) —

"(ba) downloads, distributes, transmits, disseminates, circulates, delivers, exhibits, lends for gain, exchanges, barters, sells or offers for sale, let on hire or offer to let on hire, offer in another way, or make available in any way from a telecommunications apparatus pornography"; and

(ii) by deleting the word "to" appearing immediately after the words " five years, or." in paragraph "(c)"

(b) by deleting sub clause "2" and substituting therefor the following—

(2) "It is a defence to a charge of an offence under Clause 13 (1) that a publication which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, art, representation or figure is in the interest of science, literature, learning or other objects of general concerns."

(Hon. Jennifer Shamalla)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 13 - as amended agreed to

Clauses 14 & 15 - agreed to

Clause 16 - amendment proposed –

THAT, clause 16 of the Bill be amended—

(a) by deleting the marginal note and substituting therefor the following marginal note—

"cyber harassment";

(b) in sub-clause (1) by deleting the words "and repeatedly" appearing in the opening statement;

(c) by inserting the following new sub-clauses immediately after sub-clause (3)—

"(4) A person may apply to Court for an order compelling a person charged with an offence under sub-clause (1) to refrain from—

(a) engaging or attempting to engage in; or

(b) enlisting the help of another person to engage in,any communication complained of under subsection (1);

(5) The Court—

(a) may grant an interim order; and

(b) shall hear and determine an application under subsection (4) within fourteen days.

(6) An intermediary may apply for the order under subsection (4) on behalf of a complainant under this section.

(7) A person may apply for an order under his section outside court working hours.

(8) The Court may order a service provider to provide any subscriber information in its possession for the purpose of identifying a person whose conduct is complained of under this section.

(9) A person who contravenes an order made under this section commits an offence and is liable, on conviction to a fine not exceeding one million shillings or to imprisonment for a term not exceeding six months, or to both.

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Further amendment proposed -

THAT Clause 16 of the Bill be amended by deleting sub clause (3).

(Chairperson of the Departmental Committee on Administration and National Security)

Question of the further amendment proposed;

Debate arising;

Question put and agreed to;

Further amendment proposed –

THAT clause 16 (1) of the Bill be amended by inserting the following new paragraph immediately after paragraph (b)—

"(ba) is in whole or part, of an indecent or grossly offensive nature and affects the person."

(Hon. Jennifer Shamalla)

Question of the further amendment proposed;

Debate arising;

Question put and agreed to;

Clause 16 - as amended agreed to

Clauses 17, 18, 19 & 20 - agreed to

Clause 21 - amendment proposed –

THAT, the Bill be amended by deleting clause 21 and substituting therefor the following new Clause—

Additional penalty for other offences committed through use of a computer system.

21. (1) A person who commits an offence under any other law through the use of a computer system commits an offence and shall be liable on conviction to a penalty similar to the penalty provided under that law.

(2) A Court shall, in determining whether to sentence a person convicted of an offence under this section, consider—

(a) the manner in which the use of a computer system enhanced the impact of the offence;

(b) whether the offence resulted in a commercial advantage or financial gain;

(c) the value involved, whether of the consequential loss or damage caused, or the profit gained from commission of the offence through the use of a computer system;

(d) whether there was a breach of trust or responsibility;

(e) the number of victims or persons affected by the offence;

(f) the conduct of the accused; and

(g) any other matter that the court deems fit to consider.

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 21 - as amended agreed to

Clause 22 - agreed to

Clause 23 - amendment proposed –

THAT, clause 23 of the Bill be amended—

(a) in sub-clause (7) by inserting the following new paragraphs immediately after paragraph (b) -

"(c) maintain the integrity of a computer system, any data or information accessed or retained; and
(d) maintain the confidentiality of a computer system, any data or information accessed during the execution of the warrant."

(b) in sub-clause (8) by deleting paragraph (b) and substituting therefor the following new paragraph -

"(b) compromises the integrity or confidentiality of a computer system, data or information accessed or retained under this section or misuses the powers granted under this section,
commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment not exceeding three years or to both."

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Proposed amendment withdrawn;

Further amendment proposed -

THAT, Clause 23 of the Bill be deleted and replaced by the following new clause—

Search and seizure of stored computer data.

23. (1) Where a police officer or an authorised person has reasonable grounds to believe that there may be in a specified computer system or part of it, computer data storage medium, program, data, that—

(a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence; or

(b) has been acquired by a person as a result of the commission of an offence,
the police officer or the authorised person may apply to the court for issue of a warrant to enter anypremises to access, search andsimilarly seize such data.

(2) A search warrant issued under subsection (1) shall-

(a) identify the police officer or authorised person;

direct the police officer or authorised person under

paragraph (a) to seize the data in question; or

(b) direct the police officer or authorised person to:

(i) search any person identified in the warrant;

(ii) enter and search any premises identified in the warrant; or

(iii) search any person found on or at such premises.

(3) A search warrant may be issued on any day and shall be of force until it is executed or is cancelled by the issuing court.

(4) A police officer or an authorised person shall present a copy of the warrant to a person against whom it is issued.

(Chairperson of the Departmental Committee on Administration and National Security)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 23 - as amended agreed to

Clause 24 - amendment proposed –

THAT, Clause 24 of the Bill be deleted and replaced by the following new clause-

Power to search without a warrant in special circumstances.

24 (1). A police officer or authorised person may without a search warrant search any person or premises for seizing any computer system or data referred to in section 23 -

(a) if the person to whom the search is directed consents to the search for and the seizure of any computer system or data in question; or

(b) if the police officer or authorized person on reasonable grounds believes that -

(i) a search warrant will be issued to him under section 23 if he applies for such warrant; and

(ii) the delay in obtaining such warrant would defeat the object of the search.

(2) Pursuant to Article 24 of the Constitution, this section shall limit the protection of the right to property under Article 40 of the Constitution to deprive a person of a computer system or data or of any interest in, or right over, any computer system or data to the extent contemplated under subsection (1).

(Chairperson of the Departmental Committee on Administration and National Security)

Question of the amendment proposed;

Debate arising;

Proposed amendment withdrawn;

Further amendment proposed –

THAT, the Bill be amended by deleting clause 24.

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;
Debate arising;

Question put and agreed to;

Clause 24 - deleted

Clause 25 - amendment proposed –

THAT Clause 25 of the Bill be amended-

(a) by deleting sub clause (1) and substituting therefor the following new sub clause
'(1) Where a computer system or data has been removed or rendered inaccessible, following a search or a seizure under section 23, the person who made the search shall, at the time of the search or as soon as practicable after the search make a list of what has been seized or rendered inaccessible, and shall specify the date and time of seizure.'

(b) by deleting sub clause (4).

(Chairperson of the Departmental Committee on Administration and National Security)

Question of the amendment proposed;

Debate arising;

Question put and negatived;

Clause 25 - agreed to

Clause 26 - amendment proposed –

THAT, clause 26 of the Bill be amended by-

(a) deleting sub-clause (4);

(b) deleting sub-clause (6);

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Debate arising;

Proposed amendment withdrawn;

Further amendment proposed -

THAT Clause 26 of the Bill be deleted and replaced by the following new clause—

Production order.

26. (1) Where a police officer or an authorised person has reasonable grounds to believe that-

(a) specified data stored in a computer system or a computer data storage medium is in the possession or control of a person in its territory; and

(b) specified subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control and is necessary or desirable for the purposes of the investigation,

the police officer or the authorised person may apply to court for an order.

(2) The Court shall issue an order directing -

(a) a specified person to submit specified computer data that is in that person's possession or control, and is stored in a computer system or a computer data storage medium; or

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

(Chairperson of the Departmental Administration and National Security)

Question of the further amendment proposed;

Debate arising;

Question put and agreed to;

Clause 26 - as amended agreed to

Clause 27 - amendment proposed –

THAT, clause 27 of the Bill be amended—

(a) in sub-clause (2) by deleting the words "the period specified in the notice" and substituting therefor the words "thirty days".

(b) by deleting sub-clause (4);

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 27 - as amended agreed to

Clause 28 - amendment proposed –

THAT, clause 28 of the Bill be amended-

(a) in sub-clause (4) by deleting the word "not" appearing immediately after the words "for a period";

(b) in sub-clause (7) by inserting the word "shillings" immediately after the words "ten million" appearing in paragraph (a).

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 28 - as amended agreed to

Clause 29 - amendment proposed –

THAT, clause 29 of the Bill be amended—

(a) in sub-clause (1) by deleting the words "a serious" appearing immediately after the words "in respect of" in the opening statement and substituting therefor the words "an";

(b) in sub-clause (7)(a) by inserting the word "shillings" immediately after the words "ten million".

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 29 - as amended agreed to

Clauses 30, 31 & 32 - agreed to

Clause 33 - amendment proposed –

THAT, clause 33 of the Bill be amended-

(a) in sub-clause (1) by inserting the words "the Extradition (Contiguous and Foreign Countries) Act" immediately after the phrase "2011";

(b) in sub-clause (4) by inserting the words "the Extradition (Contiguous and Foreign Countries) Act" immediately after the phrase "2011".

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 33 - as amended agreed to

Clauses 34, 35, 36 & 37 - agreed to

Clause 38 - amendment proposed –

THAT, clause 38 of the Bill be amended by deleting -

(a) the word "another" wherever it appears;

(b) the words "without the authorisation but" appearing immediately after the word "may" in the opening statement;

(c) the phrase "(open source)" appearing in paragraph (a);

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 38 - as amended agreed to

Clause 39 - amendment proposed –

THAT, clause 39 of the Bill be amended in sub-clause (2)(g) by inserting the words "to the" immediately after the word "relevant"

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 39 - as amended agreed to

Clause 40 - agreed to

Clause 41 - amendment proposed –

THAT, clause 41 of the Bill be amended in sub-clause (1) by deleting the words "and prosecuting" appearing immediately after the word "investigating".

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 41 - as amended agreed to

Clauses 42, 43, 44 & 45 - agreed to

Clause 46 - amendment proposed –

THAT, the Bill be amended by deleting Clause 46 and substituting therefor the following new clause—

PART VI—PROVISIONS ON DELEGATED POWERS

Regulations.

46. (1) The Cabinet Secretary may make regulations generally for the better carrying into effect of any provisions under this Act.

(2) Without prejudice to the foregoing, regulations made under this section may provide for—

(a) designation of computer systems, networks, programs, data as national critical information infrastructure;

(b) protection, preservation and management of critical information infrastructure;

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

(d) storage and archiving of critical data or information;

(e) audit and inspectionof nationalcritical information infrastructure;

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

(g) standard operating procedures for the conduct, search, seizure and collection of electronic evidence; and

(h) mutual legal assistance.

(3) For the purposes of Article 94 (6) of the Constitution—

(a) the purpose and objective of delegation under this section is to enable the Cabinet Secretary to make regulations to provide for the better carrying into effect of the provisions of this Act and to enable the Authority to discharge its functions more effectively;

(b) the authority of the Cabinet Secretary to make regulations under this Act will be limited to bringing into effect the provisions of this Act and to fulfill the objectives specified under this section;

Cap 2, No. 23 of 2013

(c) the principles and standards applicable to the regulations made under this section are those set out in the Interpretation and General Provisions Act and the Statutory Instruments Act, 2013.

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 46 - as amended agreed to

New Clauses 3A – 3J proposed -

THAT, the Bill be amended by inserting the following new clauses immediately after clause 3-

"PART IA – ESTABLISHMENT OF THE NATIONAL COMPUTER AND CYBERCRIMES COORDINATION COMMITTEE.

Establishment of Committee

3A. (1) There is established a National Computer and Cybercrimes Coordination Committee.

Composition of the Committee.

3B. (1) The Committee shall comprise of —

(a) the Principal Secretary responsible for matters relating to internal security or a representative designated and who shall be the chairperson;

(b) the Attorney General or a representative designated in writing by the Attorney General;

(c) the Chief of the Kenya Defence Forces or a representative designated in writing by the Chief of the Kenya Defence Forces;

(d) the Inspector-General of the National Police

Service or a representative designated in writing by the Inspector-General of the National Police Service;

(e) the Director General of the National Intelligence Service or a representative designated in writing by the Director General of the National Intelligence Service;

(f) the Director General of the Communications Authority of Kenya or a representative designated in writing by the Director General of the Communications Authority of Kenya;

(g) the Director of the Public Prosecutions or a representative designated in writing by the Director of Public Prosecutions;

(h) the Governor of the Central Bank of Kenya or a representative designated in writing by the Governor of the Central Bank of Kenya; and

(i) the Director who shall be the secretary of the Committee and who shall not have a right to vote.

(2) The Committee shall report to the Cabinet Secretary responsible for matters relating to internal security.

Functions of the Committee.

3C. (1) The Committee shall—

(a) advise the Government on security related aspects touching on matters relating to blockchain technology, critical infrastructure, mobile money and trust accounts;

(b) advise the National Security Council on computer and cybercrimes;

(c) coordinate national security organs in matters relating to computer and cybercrimes;

(d) receive and act on reports relating to computer and cybercrimes;

(e) develop a framework to facilitate the availability, integrity and confidentiality of critical national information infrastructure including telecommunications and information systems of Kenya;

(f) coordinate collection and analysis of cyber threats, and response to cyber incidents that threaten cyberspace belonging to Kenya, whether such threats or incidents of computer and cybercrime that occur within or outside Kenya;

(g) cooperate with computer incident response teams and other relevant bodies, locally and internationally on response to threats of computer and cybercrime and incidents;

(h) establish codes of cyber-security practice and standards of performance for implementation by owners of critical national information infrastructure;

(i) develop and manage a national public key infrastructure framework; and

(j) perform any other function conferred on it by this Act or any other written law.

(2) Subject to the provisions of this Act, the Committee shall regulate its own procedure.

Secretariat of the Committee.

3D. (1) There shall be a Secretariat which shall comprise of the Director and such number of public officers that, subject to the approval of the Committee, the Cabinet Secretary responsible for matters relating to internal security in consultation with the Cabinet Secretary responsible for matters relating to information, communications and technology may deploy to the Secretariat.

(2) The Director shall be-

(a) the head of the Secretariat; and

(b) responsible to the Committee for the day to day administration of the affairs of the Secretariat and implementation of the decisions arising from the Committee.

(3) Without prejudice to the generality of the provisions of subsection (4), the Director shall be responsible for-

(a) the implementation of the decisions of the Committee;

(b) the efficient administration of the Secretariat;

committee the management of staff of the Secretariat;

(d) the maintenance of accurate records on financial matters and resource use;

committee the preparation and approval of the budget for the required funding of the operational expenses of the Secretariat; and

(f) the performance of any other duties as may be assigned to him or her by the Committee.

(4) The Director shall be appointed for a single term of four years and shall not be eligible for reappointment.

Reports by the Committee etc.

3E. The Committee shall submit quarterly reports to theNational Security Council.

Critical information

3F. (1) The Director shall, by notice in the Gazette, designate certain systems as critical infrastructure.

(2) The Director shall designate a system as a critical infrastructure if a disruption of the system would result in—

(a) the interruption of a life sustaining service including the supply of water, health services and energy;

(b) an adverse effect on the economy of the Republic;

(c) an event that would result in massive casualties or fatalities;

(d) failure or substantial disruption of the money market of the Republic; and

(e) adverse and severe effect of the security of the Republic including intelligence and military services.

(3) The Director shall, within a reasonable time of designating a system as critical infrastructure, inform the owner or operator of the system the reasons for the designation of the system as a critical infrastructure.

(4) The Director shall, within a reasonable time of the declaration of any information infrastructure, or category or class of information infrastructure or any part thereof, as a critical information infrastructure, in line with a critical infrastructure framework issue directives to regulate—

(a) the classification of data held by the critical information infrastructure;

(b) the protection of, the storing of and archiving of data held by the critical information infrastructure;

(c) cyber security incident management by the critical information infrastructure;

(d) disaster contingency and recovery measures, which must be put in place by the critical information infrastructure;

(e) minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure;

(f) the period within which the owner, or person in control of a critical information infrastructure must comply with the directives; and

(g) any other relevant matter which is necessary or expedient in order to promote cyber security in respect of the critical information infrastructure.

Protection of critical information infrastructure.

3G. (1) The Committee shall within reasonable time and in consultation with the owner or a person in control of an identified critical information infrastructure, submit to the National Security Council its recommendations of entities to begazette as critical information infrastructures.

(2) The Committee shall, after the gazettement under

subsection (1), in consultation with a person that owns or operates the critical information infrastructure-

(a) conduct an assessment of the threats, vulnerabilities, risks, and probability of a cyber-attack across all critical infrastructure sectors;

(b) determine the harm to the economy that would result from damage or unauthorized access to critical infrastructure;

(c) measure the overall preparedness of each sector against damage or unauthorized access to critical infrastructure including the effectiveness of market forces driving security innovation and secure practices.

(d) identify any other risk-based security factors appropriate and necessary to protect public health and safety, or national socio-economic security; and

(e) recommend to the owners of systems designated as critical infrastructure, methods of securing their systems against cyber threats.

Reports on critical information infrastructure.

3H. (1) The owner or operator of a system designated as critical infrastructure shall report to the Committee any incidents likely to constitute a threat in the nature of an attack that amounts to a computer and cybercrime and the action the owner or operator intends to take to prevent the threat.

(2) Upon receipt of a report by Committee, under subsection (1), the National Security Council shall provide technical assistance, to the owner or operator of a critical infrastructure to mitigate the threat.

(3) The Director may institute an investigation of a computer and cybercrime attack on his or her own volition and may take necessary steps to secure any critical infrastructure without reference to the entity.

(4) The Director shall submit a report on any threat in the nature of a computer and cybercrime reported by the owners or operators of critical infrastructure periodically to the National Security Council.

Information sharing agreements.

3I. (1) A private entity may enter into an information sharing agreement with a public entity on critical information infrastructure.

(2) An agreement under subsection (1) shall only be entered into for the following purposes and in line with a critical infrastructure framework—

(a) to ensure cyber security;

(b) for the investigation and prosecution of crimes related to cyber security;

(c) for the protection of life or property of an individual; and

(d) to protect the national security of the country.

(3) Prior to the sharing of information under subsection (1) a party to an agreement shall review the information and ascertain whether the information contains personal details that may identify a specific person not directly related to a threat that amounts to a computer and cybercrime and remove such information.

(4) A person shall not, under this Part, share information relating to the health status of another person without the prior written consent of the person to whom the information relates.

Auditing of critical information infrastructures to ensure compliance.

3J. (1) The owner or person in control of a critical information infrastructure shall annually submit a compliance report on the critical information infrastructure to the Committee in line with a critical infrastructure framework in order to evaluate compliance.

(2) The Director, shall within a reasonable time before an audit on a critical information infrastructure or at any time there is an imminent threat in the nature of an attack that amounts to a computer and cybercrime, notify the owner or person in control of a critical information infrastructure in writing—

(a) the date on which an audit is to be performed; and

(b) the particulars and contact details of the person who is responsible for the overall management and control of the audit.

(3) The Director shall monitor, evaluate and report on the adequacy and effectiveness of any audit.

(4) The Director may request the owner or person in control of a critical information infrastructure to provide such additional information as may be necessary within a specified period in order to evaluate the issues raised from the audit.

(5) An owner or authorized person in control of a critical information infrastructure commits an offence and if convicted is liable to a fine not exceeding two hundred thousand shillings or term of imprisonment not exceeding five years or both if the owner or authorized person—

(a) fails to file a compliance report and fails to cooperate with an audit to be performed on a critical information infrastructure in order to

evaluate compliance with the directives issued;

(b) fails to provide such additional information as may be necessary within a specified period in order to evaluate the report of an audit in line with a critical infrastructure to the Director after he or she has been requested to do so to the Director;

(c) hinders, obstructs or improperly attempts to influence any member of the Committee, person or entity to monitor, evaluate and report on the adequacy and effectiveness of an audit;

(d) hinders, obstructs or improperly attempts to influence any person authorized to carry out an audit;

(e) fails to cooperate with any person authorized to carry out an audit; or

(f) fails to assist or provide technical assistance and support to a person authorized to carry out an audit.

(6) A person shall not perform an audit on a critical information infrastructure unless he or she-

(a) has been authorized in writing by the Director to perform such audit; or

(b) is in possession of a certificate of appointment, in the prescribed form, issued by the Director, which certificate must be submitted to the owner or person in control of a critical information infrastructure at the commencement of the audit.

(Chairperson of the Departmental Committee on Administration and National Security)

Motion made and Question proposed –

THAT, the proposed New Clauses 3A, 3B, 3C, 3D, 3E, 3G, 3H, 3I & 3J be read a Second Time

Debate arising;

Question put and agreed to;

Motion made and Question proposed -

THAT, the New Clauses 3A, 3B, 3C, 3D, 3E, 3F, 3F, 3G, 3H, 3I & 3J be part of the Bill

Question put and agreed to.

Amendment to an amendment proposed –

THAT, the proposed amendment to **New Clause 3C** by the Member for Kiambaa Constituency (Hon. Paul Koinange, M.P.) be further amended by inserting the following new paragraph immediately after paragraph (i) appearing in subclause (1)-

"(a) develop a framework for training on prevention, detection and mitigation of computer and cybercrimes and matters connected thereto"

(Hon. Dr. Patrick Musimba)

Question of the further amendment proposed;

Debate arising;

Question put and agreed to.

New Clause 12A Proposed -

THAT, the Bill be amended by inserting the following new clauses immediately after clause 12-

Publication of false information.

12A. A person who knowingly publishes information that is false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence among citizens of the Republic, or which is likely to discredit the reputation of a person commits an offence and shall on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term note exceeding ten years, or to both.

(Leader of the Majority Party)

Motion made and Question proposed –

THAT, the proposed New Clause 12A be read a Second Time

Debate arising;

Question put and agreed to;

Motion made and Question proposed -

THAT, the New Clause 12A be part of the Bill

Question put and agreed to.

New Clause 16A proposed –

THAT, the Bill be amended by inserting the following new clauses immediately afterclause 16-

Cyber terrorism.

16A. (1)A person who accesses or causes to be accessed a computer or computer system or network for purposes of terrorism, commits an offence and shall on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term note exceeding ten years, or to both.

No.30 of 2012.

(2) For the purpose of this section, "terrorism" shall have the same meaning under the Prevention of Terrorism Act, 2012.

(Chairperson of the Departmental Committee on Administration and National security)

Motion made and Question proposed –

THAT, the proposed New Clause 16A be read a Second Time

Debate arising;

Question put and agreed to

Motion made and Question proposed -

THAT, the New Clause 16A be part of the Bill

Question put and agreed to.

New Clauses 16A - 16F proposed-

THAT, the Bill be amended by inserting the following new clauses immediately after clause 16-

Cyber-squatting.

16A. A person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right, commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

Wrongful distribution of intimate images.

16B. A person who transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate image of another person commits an offence and is liable, on conviction to a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding thirty years or to both.

Identity theft and impersonation.

16C. A person who fraudulently or dishonestly makes use of the electronic signature, passwordor any other unique identification feature of any other person commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand shillings or to imprisonment for a term not exceeding three years or both.

Phishing.

16D. A person who creates or operates a website or sends a message through a computer system with the intention to induce the user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system, commits an offence and is liable upon conviction to a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding three years or both.

Interception of electronic messages

16E. A person who unlawfully destroys or aborts any electronic

or money transfers.

mail or processes through which money or information is being conveyed commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or to a term of imprisonment not exceeding seven years or to both.

Willful misdirection of electronic messages.

16F. A person who willfully misdirects electronic messages commits an offence and is liable on conviction to a fine not exceeding one hundred thousand shillings or to imprisonment for a term not exceeding two years or to both.

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Motion made and Question proposed –

THAT, the proposed New Clauses 16A, 16B, 16C, 16D, 16E & 16F be read a Second Time

Question put and agreed to;

Motion made and Question proposed –

THAT, the New Clauses 16A, 16B, 16C, 16D, 16E & 16F be part of the Bill

Question put and agreed to;

New Clauses 16A – 16H proposed -

THAT, the Bill be amended by inserting the following new clauses immediately after clause 16 -

Inducement to deliver electronic message.

16A. A person who induces any person in charge of electronic devices to deliver any electronic messages not specifically meant for him commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

Intentionally withholding message delivered erroneously.

16B.A person who intentionally hides or detains any electronic mail, message, electronic payment, credit and debit card which was found by the person or delivered to the person in error and which ought to be delivered to another person, commits an offence and is liable on conviction a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

Unlawful destruction of electronic messages.

16C. A person who unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

Wrongful distribution of

16D.A person who transfers, publishes, or disseminates, including making a digital depiction available

obscene or intimate images.

for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person commits an offence and is liable, on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

Fraudulent use of electronic data.

16E. (1) A person who knowingly and without authority causes any loss of property to another by altering, erasing, inputting or suppressing any data stored in a computer, commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

(2) A person who sends an electronic message which materially misrepresents any fact upon which reliance by another person is caused to suffer any damage or loss commits an offence and is liable on conviction a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

(3) A person who with intent to defraud, franks electronic messages, instructions, superscribes any electronic messages or instruction, commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

(4) A person who manipulates a computer or other electronic payment device with the intent to short pay or overpay commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

(5) A person convicted under subsection (4) shall forfeit the proprietary interest in the stolen money or property to the bank, financial institution or the customer.

Issuance of false e-instructions.

16F. A person authorized to use a computer or other electronic devices for financial transactions including posting of debit and credit transactions, issuance of electronic instructions as they relate to sending of electronic debit and credit messages or confirmation of electronic fund transfer, issues false electronic instructions, commits an offence and is liable, on conviction, a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

Reporting of cyber threat.

16G. (1)A person who operates a computer system or a computer network, whether public or private, shall immediately inform the Committee of any attacks, intrusions and other disruptions to the functioning of another computer system or network within twenty-four hours of such attack, intrusion or disruption.

(2)A report made under subsection (1) shall include—

(a) information about the breach, including a summary of any information that the agency knows on how the breach occurred;

(b) an estimate of the number of people affected by the breach;

(c) an assessment of the risk of harm to the affected individuals; and

(d) an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach.

(3) The Committee may propose the isolation of any computer systems or network suspected to have been attacked or disrupted pending the resolution of the issues.

(4) A person who contravenes the provisions of subsection (1) commits an offence and is liable upon conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

Employee responsibility to relinquish access codes.

16H. (1) An employee shall, subject to any contractual agreement between the employer and the employee, relinquish all codes and access rights to their employer's computer network or system immediately upon termination of employment.

(2) A person who contravenes the provision of this subsection (1) commits an offence and shall be, liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.

(Hon. Dr.Patrick Musimba)

Motion made and Question proposed –

THAT, the proposed New Clauses 16A, 16B, 16C, 16D, 16E, 16F, 16G & 16H be read a Second Time.

Debate arising;

Question put and agreed to;

Motion made and Question proposed-

THAT, the New Clauses 16A, 16B, 16C, 16D, 16E, 16F, 16G & 16H be part of the Bill.

Question put and agreed to

Schedule – amendment proposed –

THAT, the Schedule to the Bill be amended by inserting the following item in its proper sequence-

Written law	*Provision*	*Amendment*
Sexual Offences Act, 2011	16	Delete and replace with the following section-

Child pornography

16. (1) A person, including a juristic person, who knowingly—

(a) possesses an indecent photograph of a child;

(b) displays, shows, exposes or exhibits obscene images, words or sounds by means of print, audio-visual or any other media to a child with intention of encouraging or enabling a child to engage in a sexual act;

(c) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his or her possession an indecent photograph of a child;

(d) imports, exports or conveys any obscene object for any of the purposes specified in subsection (1), or knowingly or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation;

(e) takes part in or receives profits from any business in the course of which he or she knows or has reason to believe that obscene objects are, for any of the purposes specifically in this section, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation;

(f) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be produced from or through any person; or

(g) offers or attempts to do any act which is an offence under this section,

commits an offence and is liable upon conviction to imprisonment for a term of not less than six years or to a fine of not less than five hundred thousand shillings or to both and upon subsequent conviction, to imprisonment to a term of not less than seven years without the option of a fine.

(2) This section shall not apply to-

(a) Publication or possession of an indecent photograph where it is proved that such publication or possession was intended for bona fide scientific research, medical, religious or law enforcement purpose; the indecent representation of a child in a sculpture, engraving, painting or other medium on or in any ancient monument authorized by law; and

(b) activities between two persons above eighteen years of age by mutual consent.

(3) For the purposes of subsection (1) -

(a) an image is obscene if-

(i) it is lascivious or appeals to prurient interest; or

(ii) its effect, or where it comprises two or more distinct items, the effect of any one of its items, if taken as a whole, tends to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

(b) an indecent photograph includes a visual, audio or audio-visual representation

depicting-

(i) a child engaged in sexually explicit conduct;

(ii) a person who appears to be a child engaged in sexually explicit conduct; or realistic images representing a child engaged in sexual activity.

inserting the following new section immediately after section 16—

New Insert a new section immediately after section 16 as follows—

Sexual communication with a child

16A. (1) A person of eighteen years and above who knowingly communicates with a child in—

(i) a sexual manner; or

(ii) a manner intended to encourage the child to communicate in a sexual manner,

(iii) commits an offence and is liable, on conviction, to a fine of not less than five hundred thousand shillings or imprisonment for a term of not less than five years, or to both.

(2) For the purposes of this section, a communication is sexual if-

(a) any part of it relates to sexual activity, or

(b) a reasonable person would consider any part of the communication to be sexual.

(Chairperson of the Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to

Schedule - as amended agreed to

Clause 2 – amendment proposed-

THAT, clause 2 be amended -

(a) by deleting the definition of "authorised person" and substituting therefor the following new definition -

"authorized person" means an officer in a law enforcement agency or a cyber security expert designated by the Cabinet Secretary responsible for matters relating to national security by notice in the Gazette for the purposes of Part III of this Act."

(b) by deleting the definition of "Authority" and substituting therefor the following new definition -

"Authority" means the Communications Authority of Kenya";

(c) by deleting the definition of "Central Authority" and substituting therefor the following new definition -

"Central Authority" means the Office of the Attorney General";

(d) in the definition of "premises" by inserting the words "a physical or virtual space in which data is maintained, managed, backed up remotely and made available to users over a network" immediately after the word "structures";

(e) by deleting the definition of "requested state" and substituting therefor the following new definition -

"requested state" means a state being requested to provide legal assistance under the terms of this Act";

(f) by deleting the definition of "requesting state" and substituting therefor the following new definition –

"requesting state" means a state requesting for legal assistance and may for the purposes of this Act include an international entity to which Kenya is obligated";

(g) by inserting the following new definitions in the proper alphabetical sequence-

"critical information infrastructure system or data" means an information system, program or data that supports or performs a function with respect to a national critical information infrastructure;

"cybersquatting" means the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, or deprive another from registering the same, if the domain name is -

(a) similar, identical orconfusingly similar to an existing trademark registered with the appropriate government agency at the time of registration;
(b) identical or in any way similar with the name of a person other than the registrant, in case of a personal name; or
(c) acquired without right or intellectual property interests in it.

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

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

(b) significant impact on national security, national defense, or the functioning of the state.

"network" means a collection of hardware components andcomputers interconnected bycommunications channels that allow sharing of resources and information;

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

(Chairperson, Departmental Committee on Communication, Information and Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Further amendment proposed –

THAT, Clause 2 of the Bill be amended-

(a) in the definition of the word "Cabinet Secretary" by deleting the words "Information, Communications and Technology" and substituting therefor the words "internal security"

(b) by inserting the following new definition in proper alphabetical sequence -

"blockchain technology" means a digitized, decentralized, public ledger of all crypto currency transactions;

"Committee" has the meaning assigned to it under section 5;

"critical infrastructure" means the processes, systems, facilities, technologies, networks, assets and services essentials to the health, safety, security or economic well-being of Kenyans and the effective functioning of Government;

"mobile money" means electronic transfer of funds between banks or accounts deposit or withdraw funds or pay bills by mobile phone;

"trust accounts" means an account where a bank or trust company is holding funds in relation to mobile money on behalf of the public depositors;

(Chairperson, Departmental Committee on Administration and National Security)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Further amendment proposed –

Clause 2 – amendment proposed

THAT clause 2 of the Bill be amended by inserting the following definition in proper alphabetical sequence —

"pornography" includes the representation in books, magazines, photographs, films, and other media, telecommunication apparatus of scenes of sexual behaviour that are erotic or lewd and are designed to arouse sexual interest";

(Hon. Jennifer Shamalla)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Clause 2 - as amended agreed to

Long Title – amendment proposed -

THAT, the Bill be amended in the long title by inserting the words "prohibition, prevention, response," immediately after the word "detection"

(Hon. Dr. Patrick Musimba)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Long Title - as amended agreed to

Title – amendment proposed –

THAT, the title to the Bill be amended by inserting the word "misuse" immediately after the word "Computer"

(Chairperson, Departmental Committee on Communication, Information & Innovation)

Question of the amendment proposed;

Debate arising;

Question put and agreed to;

Title - as amended agreed to

Clause 1 – agreed to

Bill to be reported with amendments.

11. **HOUSE RESUMED** - the Third Chairperson in the Chair

Bill reported with amendments;

Motion made and Question proposed-

THAT, the House do agree with the Committee in the said Report

(Leader of the Majority Party)

Debate arising;

Amendment proposed –

THAT, the Motion be amended by inserting the words "subject to recommital of clauses 23 and new Clauses 16"

(The Leader of the Majority Party)

Question of the amendment deferred to another day;

12. ADJOURNMENT OF THE HOUSE TO DISCUSS A DEFINITE MATTER OF URGENT NATIONAL IMPORTANCE REGARDING DISASTERS CAUSED BY HEAVY RAINS IN THE COUNTRY

Motion made and Question proposed –

THAT, the House do now adjourn

(Hon. Alfred Keter)

Debate arising;

And the time being five minutes past One O'clock, the Third Chairperson interrupted the proceedings and adjourned the House without Question put pursuant to the Standing Orders.

13. HOUSE ROSE - at five minutes past One O'clock

M E M O R A N D U M

The Speaker will take the Chair today,
Thursday, April 26, 2018 at 2.30 p.m.

--x--