Approved
SNA
28/4/25

REPUBLIC OF KENYA

THE NATIONAL ASSEMBLY

THIRTEENTH PARLIAMENT - FOURTH SESSION - 2025

DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION

.....

REPORT ON

THE CONSIDERATION OF THE COMPUTER MISUSE AND CYBERCRIMES (AMENDMENT) BILL (NATIONAL ASSEMBLY BILL NO. 41 OF 2024)

CLERKS CHAMBERS

DIRECTORATE OF DEPARTMENTAL COMMITTEES

PARLIAMENT BUILDINGS

NAIROBI

APRIL 2025

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

CA	Communications Authority of Kenya
ICT	Information, Communication Technology
KICA	Kenya Information and Communications Act
MP.	Member of Parliament
N.A	National Assembly
KARA	The Kenya Alliance for Resident Associations

LIST OF ANNEXURES

CHAIRPERSON'S FOREWORD

This report presents the proceedings of the Departmental Committee on Communication, Information, and Innovation regarding its review of the Computer Misuse and Cybercrimes (Amendment) Bill (National Assembly Bill No. 41 of 2024). The Bill was published on 9th August 2024, read for the First Time on 25th November 2024, and referred to the Departmental Committee for consideration and reporting, in accordance with Standing Order 127.

The proposed Bill seeks to prohibit the use of electronic mediums to promote terrorism and extreme religious and cultic practices.

In compliance with Article 118(1)(b) of the Constitution and Standing Order 127(3), the Committee placed advertisements in print media on 18th February 2025, inviting comments from the public and relevant stakeholders. In response, the Committee received submissions from the Ministry of Information, Communication and the Digital Economy and the Kenya Alliance of Residents Association. The Committee held four meetings to consider the Bill and the submissions, which have been incorporated into this report.

On behalf of the Departmental Committee on Communication, Information, and Innovation, and in accordance with Standing Order 199(6), it is my privilege and honour to present this Report on the Committee's review of the Computer Misuse and Cybercrimes (Amendment) Bill (National Assembly Bill No. 41 of 2024) to the House. The Committee expresses its gratitude to the offices of the Speaker and Clerk of the National Assembly for their logistical and technical support throughout this process. We also extend our appreciation to the Ministry of Information, Communication, and the Digital Economy, as well as the various stakeholders, for their valuable contributions.

Finally, I wish to thank the Honourable Members of the Committee and the Secretariat for their insightful contributions to this report. I am pleased to report the Committee's recommendation that the Computer Misuse and Cybercrimes (Amendment) Bill (National Assembly Bill No. 41 of 2024) be approved with amendments.

Hon. John Kiarie, MP
Chairperson
Chairperson, Committee on Communication, Information and Innovation.

PART ONE

1 PREFACE

1.1 Establishment and Mandate of the Committee

1. The Departmental Committee on Communication, Information and Innovation is one of the Departmental Committees of the National Assembly established under Standing Order 216 whose mandates pursuant to the Standing Order 216 (5) are as follows:

   i. *To investigate, inquire into, and report on all matters relating to the mandate, management, activities, administration, operations and estimates of the assigned ministries and departments;*

   ii. *To study the programme and policy objectives of ministries and departments and the effectiveness of the implementation;*

   iii. *on a quarterly basis, monitor and report on the implementation of the national budget in respect of its mandate;*

   iv. *To study and review all legislation referred to it;*

   v. *To study, assess and analyse the relative success of the ministries and departments as measured by the results obtained as compared with their stated objectives;*

   vi. *To investigate and inquire into all matters relating to the assigned ministries and departments as they may deem necessary, and as may be referred to them by the House;*

   vii. *To vet and report on all appointments where the Constitution or any law requires the National Assembly to approve, except those under Standing Order 204 (Committee on Appointments);*

   viii. *To examine treaties, agreements and conventions;*

   ix. *To make reports and recommendations to the House as often as possible, including recommendations of proposed legislation;*

   x. *To consider reports of Commissions and Independent Offices submitted to the House pursuant to the provisions of Article 254 of the Constitution; and*

   xi. *To examine any questions raised by Members on a matter within its mandate.*

2. In accordance with the Second Schedule of the Standing Orders, the Committee is mandated to oversee: Communication, information, media and broadcasting (except for broadcast of parliamentary proceedings), information technology, communication technology, including development and advancement of technology, data protection and privacy, cyberspace and cyber-security, artificial intelligence, block-chain technology, and other emerging technologies.

3. In executing its mandate, the Committee oversees the Ministry of Information, Communication and the Digital Economy.

1.2 Committee Membership

4. The Departmental Committee on Communication, Information and Innovation was constituted by the House on Thursday, 27th October 2022 and further reconstituted on 6th March 2025 comprises the following Members:

Chairperson
Hon. John Kiarie Waweru, MP
Dagoretti South Constituency
UDA Party

Vice Chairperson
Hon. Alfah Miruka Ondieki, MP
Bomachoge Chache Constituency
UDA Party

Hon. Shakeel Shabbir Ahmed, CBS, MP
Kisumu East Constituency
Independent Member

Hon. Erastus Kivasu Nzioka, MP
Mbooni Constituency
WDM-K Party

Hon. Joseph Kipkosgei Tonui, MP
Kuresoi South Constituency
UDA Party

Hon. Bensuda Joyce Atieno Osogo, MP
Homabay County
ODM Party

Hon. Bernard Kibor Kitur, MP
Nandi Hills Constituency
UDA Party

Hon. Anthony Wainaina Njoroge, MP
Kieni Constituency
UDA Party

Hon. Gideon Kipkoech Kimaiyo MP
Keiyo South Constituency
UDA Party

Hon. Flowrence Jematiah Sergon, MP
Baringo County
UDA Party

Hon. Mark Ogolla Nyamita, MP
Uriri Constituency
ODM Party

Hon. Kakuta Maimai Hamisi, MP
Kajiado East Constituency
ODM Party

Hon. Khalif Ali Abdisirat MP
Nominated Member
UDA Party

Hon. Mumina Gollo Bonaya, MP
Isiolo County
Jubilee Party

Hon. Umulkher Harun Mohamed, MP
Nominated Member
ODM Party

1.3 Committee Secretariat

5. The Committee is facilitated by the following staff secretariat:

Ms. Nuri Kitel Nataan
Clerk Assistant I

Mr. Sakana Saoli
Clerk Assistant II

Mr. Thomas Ogwel
Fiscal Analyst I

Ms. Lilian Mburugu
Media Relations Officer III

Ms. Marlene Ayiro
Principal Legal Counsel I

Mr. Githinji Wanjohi
Research Officer III

Mr. Paul Shana
Sergeant At Arms

Mr. Boaz Chebiego
Research Officer III

Mr. Kelvin Lengasi
Audio Officer

Ms. Pauline Njuguna
Hansard Reporter II

Ms. Florence Wanja
Protocol Officer III

PART TWO

2 BACKGROUND OF THE COMPUTER MISUSE AND CYBERCRIMES (AMENDMENT) BILL (NATIONAL ASSEMBLY BILL NO. 41 OF 2024)

2.1 Introduction

6. The Computer Misuse and Cybercrimes (Amendment) Bill, 2024, is a Bill sponsored by Hon. Aden Daudi Mohamed, MP, the Member for Wajir East.
7. The Bill was read a First Time on 25th November 2024 and thereafter committed to the Departmental Committee on Communication, Information and Innovation to facilitate public participation pursuant to Standing Order 127.

2.2 Brief Overview of the Bill

8. The **principal object of the (Amendment) Bill** is to amend the Computer Misuse and Cybercrimes Act, CAP 79C. The Bill seeks to prohibit the use of electronic mediums to promote terrorism and extreme religious and cultic practices.

2.3 Summary of the Clauses

9. **Clause 1** provides for the short title of the Bill, to be known as the Computer Misuse and Cybercrimes (Amendment) Act, 2024.

10. **Clause 2** of the Act provides for the **Interpretation** and definition of terms. The Bill proposes to amend this section by amending one existing term and by defining some new terms in the Bill that include—

    (a) In the definition of the term **"access"** By inserting the words " through a program of a device or" immediately after the words " by a person".

    (b) by providing for new terms and their respective definitions—
    "asset" includes all property movable or immovable, physical or **virtual** and all estates, easements and rights whether equitable or legal in, over or out of property, choses-inaction, money or goodwill whether situated in Kenya or elsewhere;

Observation: The Member proposes to define the term assets that has been used in the Bill but not defined to also include "virtual assets"

"identity theft" means the use of another person's personal identification information including the name, identification number, SIM-card, bank card, bank account information, address or any other subscriber information;

"SIM-card" has the meaning assigned to it under the Kenya Information and Communications Act, 1998;

"Terrorist act" has the meaning assigned to it under the Prevention of Terrorism Act, 2012;

"Virtual account" means a digital account acquired through virtual representation.

General Observation on clause 2: It is always prudent to ensure that **all terms** used in legislation are well defined to provide for clarity in the Bill and make the Bill user friendly.

11. **Clause 3** of the Bill provides that Section 6 (of the principal Act **(On Functions of the Committee)** is amended in subsection (1) by inserting the following new paragraphs immediately after paragraph (j)—

"(ja) where it is proved that a website or application promotes illegal activities, child pornography, terrorism, extreme religious and cultic practices, issue a directive to render the website of application inaccessible;"

Observation: the law should clearly provide a criterion to be used by the committee to recommend websites to be made in accessible.
There is need to have a balance so that the provision does not contradict the provisions of Article 33 of the Constitution on Freedom of expression.

12. **Clause 4** of the Bill seeks to amend section 27 of the Act to expand the scope of the offence of cyber harassment.

13. **Clause 5** of the Bill seeks to amend Section 30 of the Principal Act is amended by-

(a) by inserting the words "or makes a call" immediately after the words "sends a message";

(b) by inserting the words "or call" immediately after the words "recipient of the message";

Observation: The proposed amendment of the Act seeks to expand the scope of the offence of (**Phishing**).

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

14. **Clause 6** of the Bill Provides for the amendment of the Principal Act by inserting the following **new** section immediately after section 42—

Unauthorized SIM-card swap. 42A. A person who wilfully causes unauthorized alteration and unlawfully takes ownership of another person's SIM-card is liable, on conviction, to a fine of not less than five hundred thousand shillings or to imprisonment for a term of not less than three years, or to both.

Observation. The Bill proposes to include a new offence of using an Unauthorised SIMCARD.

PART THREE

3 PUBLIC PARTICIPATION/STAKEHOLDER CONSULTATION

15. Following the call for memoranda from members of the public through the placement of adverts in the print media on 18th February 2025, requesting comments on the Bill and invitation of stakeholders vide letter Ref: NA/DDC/CII/2025/005 dated 20th February 2025, the Committee received submisssions from the following institutions:

    i. The Ministry of Information, Communication and the Digital Economy;
    ii. Kenya ICT Action Network (KICTANet); and
    iii. Kenya Alliance of Residents Association.

16. The stakeholders submitted as follows:

3.1 The Ministry of Information, Communication and the Digital Economy

17. The Ministry expressed support for the Computer Misuse and Cybercrimes (Amendment) Bill 2024, emphasising that it will promote the safe use of online platforms. They further informed the Committee that they are in the process of presenting a detailed review of the Computer Misuse and Cybercrimes Act, 2018, following a Stakeholder forum with proposals for amendments.
18. The Ministry submitted to the Committee a justification matrix detailing the provisions of the Bill and their intended impact, reinforcing the need for effective regulation in the industry as follows:

Table 3:1 Comments on the Computer Misuse and Cybercrimes Amendment Bill 2024

Section of the Bill	Current Text	Proposal	Justification
(a)	In the definition of the access by inserting the words through a program or a device or immediately after the words by a person; and	In addition to the proposed text, add 1. And deleting the words "and the person either ' 2. Also delete 2a 2b 2c and 2d from the definitions of the Principal Act.	The definition is criminalizing access in general and fails to distinguish between authorized and unauthorized access. The definition decriminalizes access that does not execute 2a, 2b, 2c and 2d, yet just access for sniffing purposes or reconnaissance without executing 2a. 2b, 2c and 2d is an offence.
(b)	Identity theft means the use of	Amend to read as follows:	Not all uses of personal data or entity

	another person's personal identification information, including the name, identification number, SIM card bank card bank account information, address or any other subscriber information.	"Identity theft" means the unlawful acquisition and fraudulent use of another's personal data, including the name, identification number, SIM card bankcard bank account information, address or any other subscriber information	identification information are illegal, e.g. the use of information by an employer for purposes of administration of payroll or the use of the Authority's postal address for receiving personal mail.
2 (b)	Virtual account means a digital account acquired through a virtual representation	Amend to define a digital account as opposed to a virtual account. A digital account means an electronic system that enables users to create generate send share communicate receive store display or process information providing access to digital assets.	Digital accounts encompass a wide range of online services, including email accounts, social media profiles, cloud storage services, online banking, and other platforms that store or manage digital content. On the other hand, virtual accounts are often linked to financial services and are usually operated in conjunction with primary bank accounts. Virtual accounts facilitate allocating and tracking funds within a single primary account, aiding in efficient financial management. Virtual accounts are widely used in corporate banking and treasury management. The key characteristics of digital accounts are as follows: **Electronic Access:** Digital accounts allow users to interact with digital assets through electronic means, facilitating activities such as communication, data storage, and financial transactions. **Digital Assets Management:** They serve as gateways to various digital assets, which may include; documents, multimedia files, financial records, and other forms of electronic data. **User Authentication:** Access to digital accounts typically requires authentication methods like usernames and passwords, ensuring that only authorized individuals can manage the associated digital assets.
Section 6	Section 6 of the principal Act is amended in section sub-section (1) by inserting the following new paragraph immediately after paragraph J. Ja) where it is proved that a website or application	The proposal is for the section to be deleted or enhanced to provide for a balanced approach that upholds security while	The proposed amendment to provide for the inaccessibility of applications of websites that promote illegal activities is already provided for under section 6 d which mandates the Committee to receive and act on reports relating to computer and cybercrime.

	promotes illegal activities, child pornography, terrorism, extreme religious and cultic practices, issue a directive to render the website or application inaccessible.	safeguarding fundamental human rights.	Regulating online content to effectively address cybercrime requires a balanced approach that upholds security while safeguarding fundamental human rights.
ection 27	Section 27 of the Principal Act is amended in subsection (1) by inserting the word "or is likely to cause them to commit suicide" immediately after the word "person" appearing in paragraph (b)	Amend to read: "Or cause them to commit suicide"	The proposed amendment helps to enhance the section to provide for the following: **Intentional Harassment:** The provision targets deliberate, and repeated actions intended to cause distress through electronic means, including social media, messaging platforms, emails, and other digital communications. **Causation:** Establishing a direct link between the harassment and the victim's suicide is crucial. Evidence such as communications, witness testimonies, and expert analyses may be used to demonstrate this connection. It is unlikely for one to know beforehand that what they say or do is likely to make someone else commit Suicide.
ection 27	Section 27 of the Principal Act is amended in subsection (1) by inserting the word "or is likely to cause them to commit suicide" immediately after the word "person" appearing in paragraph (b)	The scope of this proposed amendment should be expanded to cater for doxing attacks The definition of Doxing should be included under Section 2 to read as follows: Section 2 of the Computer Misuse and Cybercrimes Act is amended by inserting the following new definitions in their proper alphabetical sequence. Doxxing means the unauthorized acquisition, publication, or sharing of an individual's personal or identifying information with intent to harm, harass, or intimidate. "Sextortion" means the act of threatening to	Doxing has become a widespread cyber threat, particularly with the increasing use of social media and online platforms. The ease with which malicious actors can collect, share, and exploit personal information underscores the urgent need for robust legal measures to address these behaviors. The unauthorized sharing of personal information violates individuals' fundamental right to privacy, a principle enshrined in the Kenyan Constitution, 2010 and in the international conventions (e.g., the Universal Declaration of Human Rights, Article 12). Victims of doxxing face real threats, including stalking, harassment, and even physical harm. Including doxing in the law would enhance protections for individuals against these risks. Sextortion, a form of cybercrime where individuals are coerced into providing explicit images or engaging in sexual activities under threat of exposure, has become increasingly prevalent with the rise of digital communication platforms. Regulating sextortion is essential for several reasons: 1. **Protecting Vulnerable Populations:** Teenagers and young adults

		distribute, or distributing, intimate, sexual, or compromising images, videos, or information of an individual without their consent, with the intent to coerce that individual into providing money, sexual favors, or other benefits. Section 27 of the Principal Act is amended in subsection 1 by inserting the following new paragraphs immediately after Paragraph c d – constitutes a doxing attack f – Constitutes a sextortion attack.	are particularly susceptible to sextortion schemes. 2. **Preventing Psychological Harm:** Victims often experience severe emotional distress, anxiety, and depression. In some cases, the trauma leads to tragic outcomes, such as suicide. 3. **Deterring Criminal Activity:** Establishing clear legal consequences for sextortion acts as a deterrent. 4. **Addressing the Global Nature of the Crime:** Sextortion often involves perpetrators operating across borders, complicating law enforcement efforts. International cooperation and regulation are crucial to effectively combat these crimes. 5. **Promoting Digital Platform Accountability:** Regulation encourages online platforms to implement safeguards against sextortion. Instagram, for example, has introduced features to protect teenagers and combat sexual extortion, such as automatically blurring nudity in direct messages.
Section 27 (7)	The Court may order a service provider to provide any subscriber information in its possessions for the purpose of identifying a person whose conduct is complained of under this section	Proposal to amend this section to require the service provider to retain data logs including IP addresses and user activity logs for a minimum of 3 months from the date of use. Failure to comply to this proposed provision to lead to penalties under this Act Section 27 (7) of the Principal Act is amended by including the following provision. 27 (7A) All service providers are mandated to retain data logs, including Internet Protocol (IP) addresses and user activity logs, for a minimum duration of three (3) months from the date of each user's	This proposed amendment establishes a clear timeline for data retention to assist law enforcement agencies in carrying out investigations. This amendment aims to enhance the capacity of law enforcement agencies to investigate and prosecute cybercrimes by ensuring the availability of critical data logs. The specified retention period of three months balances investigative needs with considerations for data privacy and storage limitations. By incorporating this provision, the Act seeks to strengthen the legal framework for cybersecurity while upholding the principles of data protection and privacy.

		activity. 27 (7B) Service providers must implement appropriate technical and organizational measures to ensure the security and confidentiality of the retained data logs, preventing unauthorized access, alteration, or disclosure. 27 (7C) (1) Failure to comply with the data retention obligations stipulated in this section shall constitute an offence under this Act. (2) Upon conviction, the offending service provider shall be liable to penalties as prescribed in Section 27 (8) of this Act,	
ection 30	Section 30 of the Principal Act is amended by a) Inserting the words "or makes a call immediately after the words sends a message	Amend to read: a. Inserting the words "email or makes a call immediately after the words send a message	Phishing attacks can be executed by use of hyperlinks embedded in multimedia messages (MMS) or Rich Communication Messages (RC Messages).
ection 42	The principal Act is amended by inserting the following new section immediately after section 42. 42A – A person who willfully causes unauthorized alteration and unlawfully takes ownership of another person's SIM card with the intent to commit an offence, is liable on conviction to a fine not exceeding Kenya Shillings two hundred thousand or to imprisonment for a term not exceeding two years or both	Proposed deletion of the section.	Matters SIM card and SIM card registration are regulated under the Kenya Information and Communication Act and the Kenya Information and Communication (Registration of SIM - Card Regulations) 2015. Regulation 12 of the Registration of SIM Card Regulations, 2015, sets out the specific provision on penalties for any person who commits an offence concerning the Regulations.

19. In conclusion, the Ministry of Information, Communication and the Digital Economy submitted to the Committee that they endorsed the Bill and recommended that it be approved with proposed amendments.

3.2 Kenya ICT Action Network (KICTANet)

20. The **Kenya ICT Action Network (KICTANet)** submitted to the Committee a matrix presentation that captures their concerns and highlights their proposals on relevant provisions of each clause of the Bill. They submitted to the Committee a justification matrix detailing the provisions of the Bill and their concern, proposed recommendations as follows:

Table 3:2 The Computer Misuse and Cybercrimes (Amendment) Bill 2024 proposals

Clause No.	Provision	Issue/Concern	Proposal/Recommendation	Justification
3	Section 6 of the principal Act is amended in subsection (1) by inserting the following new paragraphs immediately after paragraph 6)— (ja) where it is proved that a website or application promotes illegal activities, child pornography, terrorism, extreme religious and cultic practices, issue a directive to render the website or application inaccessible	Lack of judicial oversight for blocking websites may lead to overreach and arbitrary censorship, infringing on digital freedoms	a) Instead of full blocking of entire websites or applications, implement more targeted measures such as blocking specific illegal content (pages, posts, or users) without shutting down entire platforms. b) Introduce judicial oversight before blocking a website or application, ensuring the National Cybercrimes Committee obtains a court order. c) Establish a partnership between the government and tech firms to co-develop regulatory frameworks that minimize disruption to services while targeting harmful content. This would also allow tech companies to offer technological solutions (like AI content filtering) to avoid full-scale blocking.	a) Proportional Blocking will minimize disruptions to legal users of websites and platforms, maintaining business continuity and reducing the ripple effects on the digital economy. This approach was seen to be effective in the European Union's Digital Services Act, where platforms must take down illegal content but not entire services. d) Judicial oversight will prevent arbitrary censorship and protect the right to freedom of expression (Article 33 of the Constitution). It also aligns with international best practices on internet governance. e) Collaborative Regulation will align

				government actions with industry practices, ensuring that both parties work towards a solution that balances cybersecurity needs with business sustainability. Involving tech firms in decision-making reduces regulatory uncertainty for developers and investors, ensuring business confidence
	Section 27 of the principal Act is amended in subsection (1) by inserting the words "or is likely to cause them to commit suicide" immediately after the word "person" appearing in paragraph (b).	The phrase "likely to cause suicide" is vague. This vagueness may lead to arbitrary enforcement where authorities could remove or penalize content that is not objectively harmful. (Article19, 2018, p. 16) Innocent online discussions, heated debates, or even controversial opinions could fall under this provision, restricting freedom of expression.	Clearly define what constitutes harmful content, and require a psychological or expert evaluation before charging someone under this provision	A clear definition of harmful content would ensure that only genuinely harmful cases are prosecuted, reducing the risk of infringing on freedom of speech and expression. This will align with the need for laws to be precise and avoid arbitrary interpretations.
	Section 30 of the principal Act is amended — by inserting the words "or makes a call" immediately after the words "sends a message"; and	The broad inclusion of all phone calls under phishing could criminalize legitimate activities like unsolicited sales calls or personal calls, even	Clarify that the amendment should target calls made with the intent to defraud or deceive the recipient, not all unsolicited calls.	This clarification will ensure that only fraudulent behavior is criminalized, protecting legitimate communication activities. It will also prevent undue burden on the justice system by reducing frivolous cases.

	by inserting the words "or call" immediately after the words "recipient of the message".	where there is no intent to defraud.		
6	The principal Act is amended by inserting the following new section immediately after section 42— 42A. A person who willfully causes unauthorized alteration and unlawfully takes ownership of another person's SIM-card with intent to commit an offense, is liable on conviction, to a fine not exceeding Kenya Shilling two hundred thousand or imprisonment for a term not exceeding two years, or to both	The proposed Section 42A poses practical implementation challenges, such as proving intent, as SIM swaps can happen for legitimate reasons. Telecom providers may face difficulties enforcing stringent identity verification without costly system upgrades, and a lack of digital forensics capacity limits law enforcement's ability to investigate. Additionally, tracking unauthorized SIM swaps may raise privacy concerns, while cross-border cases complicate enforcement. Without robust public awareness, users remain vulnerable to SIM swap fraud.	a) Mandate multi-factor authentication (MFA) for all SIM swap requests to reduce unauthorized access risks. b) Invest in Digital Forensics Training: Enhance law enforcement's capacity for digital forensics to track unauthorized SIM swaps accurately. c) Public Awareness Campaigns: Launch nationwide educational campaigns to inform users about SIM swap fraud and protection steps.	a) Multi-Factor Authentication improves security by ensuring only the legitimate owner can initiate a SIM swap, reducing the likelihood of unauthorized transfers. b) Digital Forensics Training is crucial for effective enforcement, enabling authorities to investigate and attribute unauthorized swaps to specific offenders. c) c) Public Awareness helps reduce SIM swap fraud by educating users on early signs of unauthorized access and encouraging vigilance.
General	General expansion of powers to	Broad powers to regulate and control online content can easily	Introduce periodic independent audits of the use of powers under the Act to ensure compliance with	Regular audits will enhance accountability and ensure that the law is not used to violate

	regulate online activity.	be misused without adequate checks and balances	constitutional protections of privacy and freedom of expression.	constitutional rights, fostering trust in the cybersecurity regime.

3.3 Kenya Alliance of Residents Association

21. The Kenya Alliance for Resident Associations (KARA) is an umbrella organization of resident associations in Kenya and brings together over 800 members spread across the cities, municipalities and urban areas in Kenya. KARA has established itself and contributed effectively to the attainment of better service delivery through policy advocacy and influence; capacity building; community mobilization and networking; formation and facilitation of the work of Resident Associations across the country; mediation and dispute resolutions. KARA brings together Resident Associations under one umbrella in order to strengthen their voice, and facilitate their participation in the service delivery agenda thereby enhancing social accountability both at the County & National levels.
22. The Kenya Alliance for Resident Associations (KARA) reviewed the Computer Misuse and Cybercrimes (Amendment) Bill, 2024, which is before the National Assembly and facilitated a consultative forum with non-state actors involved promotion and protection of human rights, civic space, digital rights and community dialogue and engagement.
23. The Association facilitated a Stakeholders Workshop on the Computer Misuse and Cybercrimes (Amendment) Bill 2024, from 18th and 19th February 2025 at Heron Hotel, Nairobi. The following Stakeholders participated in the workshop as presented by KARA;

Table 3:3 List of Organizations that Participated at the Stakeholders Workshop

No.	Organization	Contact Person
1.	URAIA TRUST	Nadhir Ali
2.	ACTION AID	Japheth Kitai
3.	HAKI JAMII	Valentine Mueni
4.	CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW (CIPIT)	Josephine Kaaniru
5.	AFRICA TIMES	Peace Mathoka
6.	INFORM ACTION	Steve Biko
7.	ARTICLE-19	Tracey Ishmael
8.	THE EAST AFRICAN CENTRE FOR HUMAN RIGHTS (EACHRIGHTS)	Johnstone Shisanya
9.	EMPOWER ACTION	Leah Nakami
10.	INUKA KENYA	Linet Akeyo
11.	MATHARE OASIS	Beryl Nangira
12.	UNITED DISABLED PERSONS OF KENYA	Maryanne Emomeri
13.	WANAWAKE MASHINANI INITIATIVE	Latifah Wangui
14.	AFRICA WATCH	Eddah Waithaka
15.	TPK Kenya	Festus Kiplagat
16.	KARIOBANGI SOCIAL JUSTICE CENTER	Owuor Owuor

17.	SOCIAL JUSTICE WOMEN LEAGUE	Teresiah Odock
18.	WESTMINISTER FOUNDATION FOR DEMOCRACY	Magdaline Ondieki
19.	THE EASTERN AFRICA CHILD RIGHTS NETWORK	Delphine Nyanchama
20.	RED CRAFT	James Mutua
21.	KENYA NATIONAL CIVIL SOCIETY CENTRE	Suba Churchil
22.	TRANSPARENCY INTERNATIONAL	Diana Mwanzia
23.	NATIONAL STUDENTS CAUCAS	Maxwell Magawi
24.	YOUTH SENATE KENYA	Kere Wafula
25.	THE INSTITUTE OF SOCIAL ACCOUNTABILITY	Chris Mburu
26.	ELIMU BORA	Boaz Waruku
27.	KENYA HUMAN RIGHTS COMMISSION	Martin Mavenjina
28.	YOUTH AGENDA	Brian Sengeli
29.	LAW SOCIETY OF KENYA	Christine Akinyi
30.	CIVIL SOCIETY FREEDOMS/PEN KENYA	Michelle Mwalesa
31	INTER RELIGIOUS COUNCIL OF KENYA	Rolex Mwamba
32.	CRECO Kenya	Johnstone Changwony

24. The Association supports the initiative by Hon. Mohamed Aden Daudi, MP. Whereas the Bill provides for mechanism for enhancing the Computer Misuse and Cybercrimes Act, Cap 79C, there are several areas in the Bill that KARA proposes to be amended in order to strengthen the legislative measures proposed. In addition, KARA proposes further amendments to the Act that should be included in the Bill as highlighted below:

25. THAT **Clause 2** of the Bill be amended as follows–

(a) In paragraph (a) by deleting the proposed word "or" appearing after the word "devise"

(b) In paragraph (b) by inserting the words "password" after the word after the word "address"

Justification

The proposed word "or" in paragraph changes the meaning of definition of the word "access" since it would imply. With the proposed amendment under paragraph (a), the definition of the term "Access" would read as follows: "access means gaining entry into or intent to gain entry by a person through a program or a devise or to a program or data stored in a computer system and the person either.....". This changes the meaning of the clause since the purpose of using a devise is to gain access to a program or data.

Passwords are considered as personal data that is linked to an identifiable person since it is used to access a person's personal accounts or information. Therefore, they should be included in the definition of identity theft.

26. **THAT Clause 3** of the Bill be amended by deleting the proposed paragraph (ja) and substituted therefor the following–

(ja) coordinating public and private sector entities in monitoring and preventing computer misuse through the propagation of criminal activities such as child pornography, production, supply or sale of narcotic drugs and controlled psychotropic substances, terrorism, organized crime or violent extremism as prescribed under relevant laws in Kenya.

Justification

The proposed paragraph (ja)–

(a) provides for the powers of the National Computer and Cybercrimes Coordination Committee under section 6 of the Act, whereas section deals with functions of the committee and not its powers. Consequently, its misplaced in its form and legislative flow

(b) Would be prone to abuse since it does not provide for mechanism for proving that such criminal activities before placing websites and related applications offline. The due process should be followed in all circumstances. The issue of rendering websites and other applications inaccessible should be as a consequence of a criminal conviction under the relevant laws.

27. **THAT** the **Bill be amended by inserting a new clause 3A** as follows–

3A. The Principal Act is amended in section 5 (1) by inserting new paragraphs (k) and (l) as follows–

(k) the Data Commissioner;

(l) the chairperson of the Kenya National Commission on Human Rights; and

(m) the Chairperson of the National Council for Persons with Disability.

Justification

Data privacy and protection as well as human rights are closely related to computer misuse and cybercrimes in terms of breaches and enforcement processes. Therefore, there is need to have the Data Commissioner and Chairperson of Kenya National Commission on Human Rights as members of the Committee. In addition, it would be important to include persons with disability in the committee to ensure that issues affecting persons with disability are integrated in control of computer misuse and cybercrimes.

28. THAT **the Bill be amended in Clause 4** by inserting the words "inflict any self-physical harm or injuries" after the word "suicide"

Justification

It would be appropriate in include other negative effects that may affect an individual as a result of cyber harassment such physical harm.

29. THAT **Clause 6 of the Bill be deleted**.

Justification

The proposed Clause 42A is misplaced as it seeks to provide for a crime whose subject matter falls under the Kenya Information and Communication Act, Cap 411A. Specifically, matters SIM Cards are covered under sections 27A, 27B, 27C and 27D. Consequently, control of SIM- Card Swap should be covered under this part dealing with SIM-Card registration and management. In addition, provision of unauthorised SIM-Card Swap as a crime under the Computer Misuse and Cybercrimes Act creates an opportunity for the same offence being regulated under 2 Acts, which would be a miscarriage of justice.

30. THAT **the Bill be amended by inserting a new Clause 7** as follows–

The Principal Act is amended by inserting a new section 46A as follows–

46A. (1) Where a person has been convicted of an offence related to child pornography, production, supply or sale of narcotic drugs and controlled psychotropic substances, terrorism, organized crime or violent extremism as prescribed under relevant laws in Kenya, and the person was using a computer system, website or digital device in contravention with this Act, the court may order the person to–

a. remove the content or materials from the computer system, website or digital device;
b. close or deactivate the computer system, website or digital device; or
c. such other orders as the court may deem appropriate.

(2) Notwithstanding subsection (1), an authorised person may, where the person believes that a person is committing crimes described under subsection (1) using a computer system, website or digital device, the authorised officer may apply to court for order that the person–

(a) removes the content or materials from the computer system, website or digital device;
(b) closes or deactivates the computer system, website or digital device; or
(c) such other orders as the court may deem appropriate.

Justification

The proposed section 46A will address the need to close websites and applications that are used to commit the crimes described under clause 3 of the Bill. The proposed section 46A will ensure that there is fair and accountable administrative system in regard to closing websites or digital applications.

31. THAT the Act be amended by reducing all fines stipulated under section 14 (Unauthorised access), 15 (Access with intent to commit further offence), 22 (false publications), 23 (publication of false information), 27 (cyber harassment) and any other section who's fine is above Ksh. 500,000 or imprisonment of more than 2 years to the extent that such penalties relate to individuals, from the stipulated amounts to not more than Ksh. 200,000.

Justification

The Act has been used to target persons deemed to be critics of the government or persons in positions of power. This has resulted in the Act being deemed to focus less on controlling computer misuse and cybercrimes and more on political control and eventual curtailment of freedom of speech, media, and expression. Hefty fines such as Ksh. 5, 10, or 20 million would be deemed to inhibit such freedoms by instilling fear due to misinterpretation of the law.

PART FOUR

4 COMMITTEE OBSERVATION

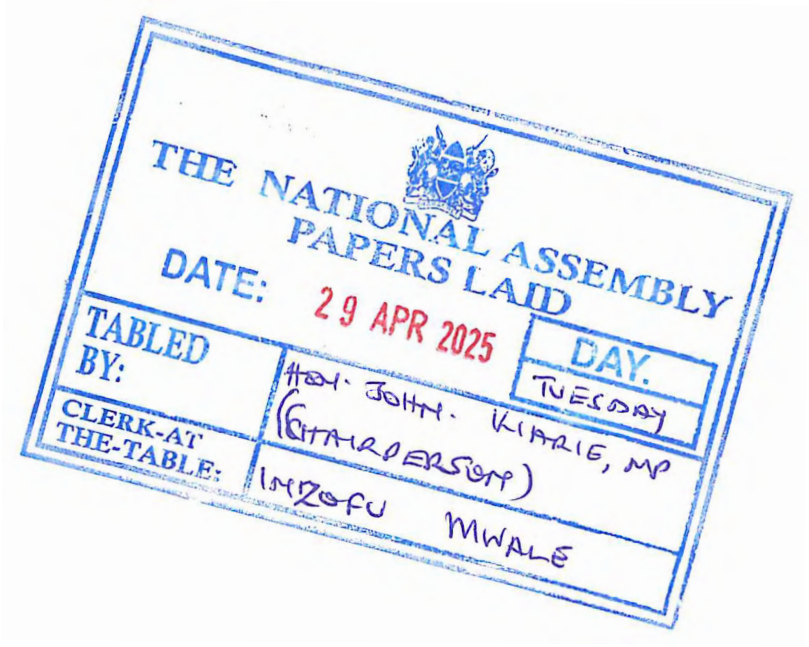
32. The Committee made the following observations from the public participation and stakeholder engagement:

    i. The Ministry of Information, Communication, and the Digital Economy needs to develop a national cybersecurity policy to address growing cyber threats and establish a national cybersecurity agency to serve as Kenya's primary cybersecurity point of contact; and
    ii. That there is a need to strengthen already existing laws on defamation to deal with issues of cyberbullying as opposed to amending the Computer Misuse and Cybercrimes Bill.

PART FIVE

5 COMMITTEE RECOMMENDATION

33. The Committee having considered the Computer Misuse and Cybercrimes Bill *(National Assembly Bill No. 41 of 2024)*, recommends that the House **approves** the Bill with amendments.



PART SIX

6 SCHEDULE OF PROPOSED AMENDMENTS

34. The Committee proposed the following amendments to be considered by the House at the Committee Stage—

CLAUSE 2

THAT clause 2 of the Bill be amended—
(a) in paragraph (a) by deleting the word "or" appearing immediately after the word "device"; and
(b) in paragraph (b) by—
(i) inserting the word "password" immediately after the word "address" in the proposed definition of the word "identity theft";
(ii) deleting the definition of "SIM-card"; and
(iii) inserting the following new definitions in their proper alphabetical sequence—
"Computer misuse" refers to the unauthorized use, modification or access to a computer system, program or data; and
"cybercrime" refers to an offence committed through the use of information and communication technology to target networks, systems, data, websites or technology or to facilitate a crime.

Justification— The word "or" appearing immediately after the word "device" in the definition of "access" changes the meaning of the clause since the purpose of using a device is to gain access to a program or data.

The inclusion of the word "password" in the definition of "identity theft" is necessary as a password is considered personal data that is linked to an identifiable person since it is used to access a person's personal account or information.

The deletion of the word "SIM-card" is necessary as the word will not be used in the Bill and Act after deletion of the proposed clause 6 of the Bill which seeks to introduce a new section 42A on unauthorised SIM-card swap.

The words "computer misuse" and "cybercrime" have not been defined in the Act despite being used severally in the Act.

CLAUSE 5

THAT clause 5 of the Bill be amended—
(a) in paragraph (a) by inserting the words "email or" immediately after the word "or"; and
(b) in paragraph (b) by inserting the words "email or" immediately after the word "or".

Justification—Phishing attacks can be executed by use of hyperlinks embedded in multimedia messages (MMS) or Rich Communication Messages (RC Messages).

CLAUSE 6

THAT the Bill be amended by deleting clause 6 and substituting therefor the following new clause—

6. The principal Act is amended by inserting the following new section immediately after section 46—

Insertion of a new section 46A in Cap 79C.

Further court orders.

46A. (1) Where a person has been convicted of an offence related to promotion of illegal activities, child pornography, terrorism, extreme religious and cultic practices and the person was using a computer system, website or digital device in contravention of this Act, the court may—

(a) order the person to remove the content or materials from the computer system, website or digital device;

(b) order the person to close or deactivate the computer system, website or digital device; or

(c) make such orders as the court may deem appropriate.

(2) Notwithstanding subsection (1), where an authorised person believes that a computer system, website or digital device is being used to promote illegal activities, child pornography, terrorism, extreme religious and cultic practices, the authorised person may apply to court for—

(a) an order for removal of the content or materials from the computer system, website or digital device;

(b) an order for closure or deactivation of the computer system, website or digital device; or

(c) such orders as may be necessary.

Justification—Clause 6 proposes to introduce a new clause 42A to provide that unauthorised SIM-card swap is a crime. However, SIM-cards registration, use and related crimes are covered under sections 27A, 27B, 27C and 27D of the Kenya Information and Communications Act, Cap 411A. Therefore, the proposed clause 6 should be deleted to avoid an instance where the same offence is regulated under two different Acts, which would be a miscarriage of justice.

The proposed insertion of a new section 46A ensures that the Court will have power to order removal, closure, deactivation or inaccessibility of websites, computer systems or digital devices that promote terrorism and extreme religious and cultic practices.

SIGNED.....DATE 24 APRIL 2025

HON. JOHN KIARIE, MP
CHAIRPERSON
DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION

THIRTEENTH PARLIAMENT - FOURTH SESSION – 2025

DIRECTORATE OF DEPARTMENTAL COMMITTEES

DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION

ADOPTION SCHEDULE

Report on the consideration of the Computer Misuse and Cybercrimes (Amendment) Bill (NA Bill No. 41 of 2024)

No.	MEMBER	SIGNATURE
1.	Hon. John Kiarie Waweru, MP - **Chairperson**	
2.	Hon. Alfah Miruka Ondieki, MP – **Vice Chairperson**	
3.	Hon. Shakeel Shabbir Ahmed, CBS, MP	
4.	Hon. Erastus Kivasu Nzioka, MP	
5.	Hon. Joseph Kipkosgei Tonui, MP	
6.	Hon. Bensuda Joyce Atieno Osogo, MP	
7.	Hon. Bernard Kibor Kitur, MP	
8.	Hon. Geoffrey Wandeto, MP	
9.	Hon. Gideon Kimaiyo Kipkoech, MP	
10.	Hon. Flowrence Jematiah Sergon, MP	
11.	Hon. Irene Nyakerario Mayaka, MP	
12.	Hon. Kakuta Maimai Hamisi, MP	
13.	Hon. Khalif Ali Abdisirat, MP	
14.	Hon. Mumina Gollo Bonaya, MP	
15.	Hon. Umulkher Harun Mohamed, MP	