KICTANet
The Power of Communities

MEMORANDUM ON:

THE COMPUTER MISUSE AND CYBERCRIMES (AMENDMENT) BILL 2024

Submitted to:
Clerk of the National Assembly

Submitted By:

Kenya ICT Action Network (KICTANet)

08 October 2024

Cover Letter

8 October 2024,

Clerk of the National Assembly,
Main Parliament Buildings, Nairobi,
P.O. Box 41842-00100,
Nairobi

Submitted via email to cna@parliament.go.ke

Dear Sirs,

Re: Memorandum on The Computer Misuse and Cybercrimes (Amendment) Bill 2024

Greetings from KICTANet!

We submit this memorandum with expertise on human rights and Information and Communication (ICTs).

We submit this memorandum in response to the call for input on The Computer Misuse and Cybercrimes (Amendment) Bill 2024.

We have included herein a matrix presentation that captures our concerns, and highlights our proposals on relevant provisions of each of the Bills for your review and consideration. We would be glad to provide further input and perspectives on the Bills, as and when required.

We have included herein a matrix presentation that captures our concerns, and highlights our proposals on relevant provisions of the Bills for your review and consideration. We would be glad to provide further input and perspectives on the Bill, as and when required.

We look forward to your response.

Regards,

Kenya ICT Action Network (KICTANet)

1. **The Computer Misuse and Cybercrimes (Amendment) Bill 2024**

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.[1]	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	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.[2] b) 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.

[1] Victor K. (2024, October 3). Proposal to Block Websites and Applications Threatens Kenya's Digital Ecosystem | KICTANet Think Tank

[2] DSA Observatory. (2021, July 27). The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations - DSA Observatory, also Article 8 of the EU Digital Services Act

Clause No.	Provision	Issue/Concern	Proposal/Recommendation	Justification
			content filtering) to avoid full-scale blocking.	c) 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.
4	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	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.[3] This will align with the need for laws to be precise and avoid arbitrary interpretations.[4]

[3] Article 24 of the Constitution of Kenya

[4] Sugow, A., Zalo, M., & Rutenberg, I. (2021). Appraising the impact of Kenya's cyber-harassment law on the freedom of expression. JIPIT: Journal of Intellectual Property and Information Technology Law, 1(1), 91-114

Clause No.	Provision	Issue/Concern	Proposal/Recommendation	Justification
		controversial opinions could fall under this provision, restricting freedom of expression.		
5	Section 30 of the principal Act is amended — by inserting the words "or makes a call" immediately after the words "sends a message"; and by inserting the words "or call" immediately after the words "recipient of the message".	The broad inclusion of all phone calls under phishing could criminalize legitimate activities like unsolicited sales calls or personal calls, even where there is no intent to defraud.	Clarify that the amendment should target calls made with the intent to defraud or deceive the recipient, not all unsolicited calls.[5]	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.
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 to	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	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.	a) Multi-Factor Authentication improves security by ensuring only the legitimate owner can initiate a SIM swap, reducing the likelihood of unauthorized transfers.[6] b) Digital Forensics Training is crucial for effective enforcement, enabling authorities to investigate

[5] Refer to Sections 310.3 and 310.4 of the USA FTC's Telemarketing Sales Rule, which specifically help separate permissible business practices from phishing or fraudulent actions based on clear prohibitions against deception, unauthorized billing, and misrepresentation.
[6] Scheidel, J. (n.d.). Preventing SIM Swap Scams with Biometric Multi Factor Authentication. authID

Clause No.	Provision	Issue/Concern	Proposal/Recommendation	Justification
	imprisonment for a term not exceeding two years, or to both.	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	c) Public Awareness Campaigns: Launch nationwide educational campaigns to inform users about SIM swap fraud and protection steps.	and attribute unauthorized swaps to specific offenders.[7] c) Public Awareness helps reduce SIM swap fraud by educating users on early signs of unauthorized access and encouraging vigilance.[8]
General	General expansion of powers to regulate online activity	Broad powers to regulate and control online content can easily be misused without adequate checks and balances.	Introduce periodic independent audits of the use of powers under the Act to ensure compliance with constitutional protections of privacy and freedom of expression.	Regular audits will enhance accountability and ensure that the law is not used to violate constitutional rights, fostering trust in the cybersecurity regime.[9]

[7] Daniel Artasasta Tambunan, Suryadi MT, Supardi hamid, Cyber Policing In Preventing Sim Swap Attacks, A New Threat To Digital Economy Transactions, Management Technology and Security International Journal, pg 135 - 136
[8] Ibid
[9] House of Lords Select Committee on Communications. (2019). *2nd report of session 2017–19:* Regulating in a digital world
Memorandum on The Computer Misuse and Cybercrimes (Amendment) Bill 2024