December 3, 2023

The Chairperson,
Policy and Legislative Reform Working Group for
Information, Communication and Digital Economy Sector
Ministry of Information, Communication and the Digital Economy,
P.O Box 30025-80100
Nairobi

Dear Sir,
RE: Memorandum on The Kenya Information and and Communications Act, 1998 and the Computer Misuse and Cybercrimes Act 2018.

Greetings from KICTANet.

KICTANet is a multistakeholder think tank for ICT policy and regulation. Its guiding philosophy encourages synergies for ICT policy-related activities and initiatives. KICTANet's overall mission is to promote an enabling environment in the ICT sector that is robust, open, accessible, and rights-based. Its strategic objectives during 2022 - 2024 are effective multistakeholder participation; promoting an enabling environment; building capacities and empowered communities; and institutional strengthening.

We submit this memorandum in response to the request for contributions for the reform of the information, communication and digital economy sector.

We have included herein a matrix presentation that captures our concerns and highlights our proposals on relevant provisions of the Kenya Information and Communications Act, 1998 and the Computer Misuse and Cybercrimes Act 2018 for your review and consideration.

We would be glad to provide further input and perspectives on our suggestions and recommendations, as and when required. We look forward to your response.

Sincerely,

Grace Githaiga

Grace Githaiga,
Convener, KICTANet

Nine Planet Apartments, Unit E9, Kabarnet Gardens Road, Nairobi, Kenya
+254 722 701495 | info@kictanet.or.ke
| www.kictanet.or.ke

Proposals on relevant provisions of the Kenya Information and Communications Act, 1998				
Section	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
2	This section does not provide for the definition of the various forms of online gender based violence including: cyberbullying, non-consensual sharing of intimate images, doxing, cyber stalking, domestic surveillance, online shaming, trolling and cyber harassment	Gender based violence has been adopted on the online space. OGBV takes different forms which need to be defined in order to hold perpetrators accountable and regulate online behavior.	In defining these terms, it is important to strike a balance. It will be important to avoid overly broad definitions that may invite ambiguity and misinterpretation, on the other hand, overly narrow definitions might hinder the adaptability of laws to future offence. Clarity and objectivity should be key considerations when defining these offences.	Concise definitions provide a clear legal framework to address and prosecute such offences. Gives guidance to law enforcement hence enabling proper investigation and presentation of evidence. Perpetrators can be held accountable. Act as a deterrent of OGBV.
29	This section provide for the offence of using a telecommunication system to: send grossly offensive/ indecent/ obscene messages or false messages that cause annoyance, inconvenience or anxiety	The ingredients of these offences are too wide hence the potential for misinterpretations by courts. Perpetrators may rely on the ambiguity in law to their advantage.	More concise definitions. Set the parameters that an act or omission should meet in order to constitute an offence.	Precision ensures an effective legal framework. Precision guides victims of OGBV and law enforcement on how to present evidence.
84D	This section provides for the offence of publishing *obscene information* in electronic form.	There is no definition in the Act of what constitutes *"obscene information"*. A wide interpretation of this section could be used to prosecute cases of non-consensual sharing of intimate images or cyber-flashing. Precision is important because as currently worded this	This section should be made more precise and offences such as non-consensual sharing of intimate images and cyber-flashing should be included in this section.	Perpetrators may rely on ambiguity of the section to avoid consequences. Inclusion of the offences of non-consensual sharing of intimate images and cyber-flashing will be reflective of the

		offence is very subjective and ambiguous.		current circumstances.
		Provision of other forms of remedies to victims of OGBV. The offences in the Act attract either a jail term or fine against a perpetrator, however OGBV victims often suffer emotional, psychological and sometimes financial losses. These losses should be adequately be compensated	Inclusion of protection orders to protect victims from further risk of abuse. Provision of monetary damages to the victim to compensate them for emotional, psychological and financial losses suffered or to enable them seek psycho-social rehabilitation.	Victims of OGBV need to be protected and also, in the best possible extent, be reinstated to the lives they enjoyed prior to the abuse. Thus compensation to enable them seek therapy or for financial losses suffered is imperative.
		Procedure of seeking orders including protection orders. Due to the nature of the online space, harmful and abusive content tend to spread very fast and to a wide audience hence it is necessary to deal with such cases expeditiously.	The Act should provide for protection orders where necessary, on an *ex parte* basis.	This will protect victims of OGBV from the continuous spread of harmful and abusive content pending the hearing and determination of the main case.
		Clear parameters for intermediary liability. OGBV cases reported to ISPS and platform owners in Kenya are not being addressed adequately.	To uphold the right to freedom of expression the Act should provide clear procedures for holding intermediaries liable for content posted by users. This should only occur where the intermediary refuses to obey a court order to remove harmful and abusive content.	It is imperative that a balance is struck between upholding the right to freedom of expression and protecting women and girls from OGBV. Where an intermediary refuses to take down harmful and abusive content, victims should have a remedy in court.
		Separate registration of SIM cards belonging to children	The Act should make provisions that require service providers to register SIM cards used	Girls are vulnerable on the online space therefore it is

			by children separately and to filter content to such SIM cards and provide tools to parents and schools for child protection.	imperative that extra measures are put in place to protect them through ISPs and telecommunicatio n providers.
		Anonymity of perpetrators of OGBV often stands in the way of victims getting justice.	The Act should establish processes to identify anonymous perpetrators i.e. by linking digital identifiers such as IP addresses to physical devices. Such an identification process should be done after obtaining approval from the court. The order should comply with due process and Article 24 with respect to legality, legitimate purpose, necessity and proportionality as grounds for limitation of fundamental right to privacy.	Perpetrators of OGBV rely heavily on anonymity to initiate and continue harm and abuse. It is therefore imperative that necessary measures are put in place to unmask the perpetrator.
		Mutual legal assistance for extraterritorial reach. In some circumstances perpetrators are not within the jurisdiction of Kenya.	The Act should establish a framework for international cooperation to assist victims of OGBV to get remedies against perpetrators who are not resident in Kenya.	A framework for mutual legal assistance within the KICA Act is necessary to ensure that all perpetrators under the Act face the consequences of their actions regardless of their geographical locations.

COMPUTER MISUSE AND CYBERCRIMES ACT, 2018

Section	Provision	Issue/ Concern	Proposal/Recommendation	Justification for Proposal
~~3 (d) Objects of the Act~~ 2	~~States that the Act seeks to protect the rights to privacy, freedom of expression and access to information as guaranteed in the Constitution~~ This section does not define technology facilitated gender-based violence that is through computer systems and networks. It also does not provide for and define the various forms of OGBV including: cyberbullying, non-consensual sharing of intimate images, doxing, cyber stalking, domestic surveillance, online shaming, trolling and cyber harassment	The omission of explicit reference to online gender-based violence may be addressed by proposing an amendment that explicitly recognizes and addresses this issue which has become rampant.	Include a specific clause that addresses online gender-based violence and harassment, emphasizing the protection of women's safety and rights in digital spaces	Incorporating this amendment would strengthen the Act's commitment to safeguarding the rights and safety of all individuals, with a particular focus on mitigating the risks faced by women in the online sphere as addressed in some of the sections.
5 (1) Composition of the committee.	The section outlines the composition of the National Computer and Cybercrimes Co-ordination Committee (NC4). ~~different institutions and what the committee of the National Computer and Cyber Crimes Coordination Committee shall comprise of~~	The committee does not include a representative from the National Gender and Equality Commission (NGEC) and a ~~gender~~ representative and the Office of the Data Protection Commissioner which was established after this Act.	The section should be amended ~~and add a gender national institutional representative or institution such as the~~ to include a representative of the National Gender and Equality Commission to the National Computer and Cybercrimes Committee to advise on the gender-specific cyber threats ensuring inclusive	Online-gender based violence has become a pervasive issue in the digital space. By incorporating these recommendations the National Computer and Cyber Crimes Coordination Committee can better address the multifaceted challenges posed by OGBV and enhance its overall effectiveness in safeguarding digital spaces and align with international standards

			and effective policies. Include a representative from the Office of the Data Protection Commissioner to ensure a holistic approach to cybersecurity as it is closely tied to cybercrimes.	recognizing gender representation in cybersecurity. This shall also prevent overlapping of functions.
6 Function of the National Computer and Cybercrimes Co-ordination Committee	The functions of the National Computer and Cybercrimes Co-ordination Committee ~~Computer Misuse and CyberCrimes Act~~ currently lacks explicit mention of a dedicated focus on gender-specific cyber threats and aspects raising concerns of its ability to comprehensively address online-gender based violence which might be overshadowed if not expressly indicated.	Without a specific focus on gender, there's a risk of overlooking the unique challenges faced by individuals particularly women in the context of cybercrimes such as non-consensual sharing of intimate images, image-based abuse, tech-facilitated sexual exploitation and abuse as well as sextortion which is currently rampant.	Introducing a function dedicated to gender-related aspects ensures the committee actively addresses issues such as online-gender based violence, providing a more inclusive approach	This aligns with the commitment to protect all rights irrespective of gender as outlined under Article 27 of the Constitution of Kenya, 2010
37 Wrongful distribution of obscene and intimate images	The Act addresses the offense of wrongful distribution of obscene and intimate images	While it might cover images, the absence of specifically including videos unless fished out of other sections of this act creates ambiguity potentially leaving a gap in protection against non-consensual sharing of intimate videos.	Specify and explicitly include or add the wrongful distribution of obscene and intimate images and videos ensuring a comprehensive approach to combating the non-consensual sharing of explicit content.	By specifying and including the forms of online-gender based violence by their specific names in this case; the wrongful distribution of obscene and intimate videos in legal provisions, the act becomes more adaptive, encompassing technological changes or even AI

				altered videos providing more protection against ever evolving cybercrimes
48, Search and seizure of computer stored data 49. Record of and access to seized data	The sections highlights the investigative procedures in search and seizure of computer stored data, record of and access to the seized data	Inadequate safeguards for protecting the privacy of individuals, particularly addressing gender-related information/data during cybercrime investigations such as sensitive data ~~should be specified~~.	Ensure law enforcement receives training on gender-sensitive investigative techniques to handle sensitive information with discretion. Establish clear protocols for the seizure of data, emphasizing the need to respect privacy rights, especially in cases involving gender-related data.	Safeguarding the privacy of individuals is fundamental, especially when dealing with sensitive data that may involve gender-related information. Training ensures that investigators approach cases without biases and handle gender-related data with sensitivity and professionalism. Implementing these recommendations can strike a balance between effective cybercrime investigations and protecting individuals' privacy, specifically addressing gender-related concerns in compliance with data protection principles.