Strathmore University

Centre for Intellectual Property and Information Technology Law

Comments on the International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

The Center for Intellectual Property and Information Technology (CIPIT), based in Nairobi, Kenya is a is a think tank and training Centre established under Strathmore University. The scope of work includes evidence-based research and training in intellectual property, information technology law, and policy. CIPIT commends and supports the efforts of the Adhoc Committee in developing a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. CIPIT further applauds the AdHoc Committees' multi-stakeholder approach in developing an effective and comprehensive framework addressing cybercrime while upholding the protection of human rights.

This submission reflects CIPIT's contribution to the ongoing negotiation processes in consideration of the already established national laws on cybercrime in Kenya i.e. the Computer Misuse and Cybercrimes Act No 5 of 2018 that form a foundational basis for furtherance of the provisions of the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Chapter	Article	Recommendation/ Comment	Justification
Chapter I - General Provisions	2 (a) "[Computer system] [Information and communications technology device]";	Provide meaning to [Information and communications technology device]"- refers to any electronic device or equipment that is capable of processing,	These devices collectively form the foundation of modern technological infrastructure, enabling individuals, businesses, and governments to communicate, access

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034612
Email: cipit@strathmore.edu Website:www.cipit.strathmore.edu

		transmitting, receiving, or storing digital information. They encompass a wide range of technologies and tools that enable the exchange of data and facilitate communication over digital networks. ICT devices can include, but are not limited to computer systems, servers, storage devices, communication devices, and embedded systems,	information, and conduct various activities efficiently. However, their widespread use also introduces challenges related to cybersecurity, privacy, and the potential for misuse in criminal activities.
	Personal Data	Expound on the definition of personal data to mean, 'any data relating to an identified or identifiable natural person' data protection.	Inserting the addition of 'any' ensures the scope of personal data can be broadly interpreted. This is noting the continuous evolution of technology and the extent to which personal data can be used or the mediums within which it can be present and can directly or indirectly identify and individual.
	Addition -	Definition of Child Sexual Abuse and Child Exploitation Material	Child sexual abuses and child exploitation material are offenses listed under Article 13 however no particular definitions are ascribed to both

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034612
Email: cipit@strathmore.edu Website:www.cipit.strathmore.edu

			offenses. The definition of Child sexual abuse varies from jurisdiction to jurisdiction and is subject to state party interpretation and definition as prescribed by national laws. For instance the Kenyan Children Act 2022 defines Child abuse but not Child Sexual abuse further there is no given definition or description of what comprises child exploitation material.
Chapter II- Criminalization	17- Offences relating to other international treaties "States Parties shall adopt such legislative and other measures as may be necessary to ensure that offenses established in accordance with applicable international Conventions and protocols that also apply when committed through the use of [a computer system] [an information and communications technology device]."	Add the following clause: "State parties shall adopt technologically neutral language related to international treaties"	The provision emphasizes the need for harmonizing national legislation with applicable international Conventions and protocols. This ensures that cyber-enabled offenses are treated with the same seriousness and legal consequences as traditional crimes, fostering a unified approach to addressing global challenges posed by cybercrime. The provision's language underscores the principle of technological neutrality, which

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034612
Email: cipit@strathmore.edu Website:www.cipit.strathmore.edu

			means that legal definitions and consequences are not tied to specific technologies but rather to the nature of the offense itself. This is essential in ensuring that legal frameworks remain relevant as technology continues to evolve.
Chapter IV - Procedural Measures and Law Enforcement	**Defining Competent Authority**	Provide the definition of Competent Authority in consideration of states that may already have existing competent authority established through national laws. The Definition should also encompass the undertakings of the statutory authority as highlighted in various articles in the draft i.e Articles 12 (b), 40(4), 49 (2b)	Competent authorities handling cyber security matters that may vary. They could be identified as Criminal Justice Agencies, National Security Agencies, Private Sector or Public-Private Partnerships and Task Forces. These vary from jurisdiction to jurisdiction and each of these authorities may in different capacities have different purposes for which investigations are carried out. Establishing an independent competent authority guarantees impartiality and a well-established channel through which complaints and investigations can be carried out independent of any underlying interests. Further, the authority will have

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034612
Email: cipit@strathmore.edu Website:www.cipit.strathmore.edu

			specialized knowledge facilitating the effective prevention, mitigation, detection, investigation, prosecution, and adjudication with clear standards of procedure having established clear enforcement mechanisms, particularly in establishing enforcement mechanisms of the provisions of Article 34. In line with this, this would further establish a system through which the 24/7 network is established as provided under Article 41. Additionally, this would open up the world to a creation of a global agency comprised of all competent authorities existing across the different state parties facilitating easy decision-making on matters of jurisdiction and extradition as prescribed under Chapter III as well as strengthening international cooperation.
Chapter V - International Cooperation	**Article 36 Protection of Personal Data**	Include provisions for state parties that lack personal data protection laws explicitly stating the lack of transfer of	The provisions on the protection of personal data presume that all state parties have enacted data protection

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034612
Email: cipit@strathmore.edu Website:www.cipit.strathmore.edu

		any personal data where countries lack data protection laws. Alternatively, state the application of Convention 108 where countries lack data protection laws but have ratified the Convention.	laws which is not the case. From an African Perspective, 34 out of the 54 countries have established data protection laws. This will, therefore, limit the application of the Convention particularly where countries that lack data protection laws may be required to transfer personal data in accordance with the Convention.

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034612
Email: cipit@strathmore.edu Website:www.cipit.strathmore.edu