Regional Conference on Africa Child Online Protection (ACOP)

Empowering the future digital citizens

Kampala, Uganda

15-16 December 2014

African Union Perspectives on Cybersecurity and Cybercrime Issues.

The AU Convention on Cyber Security and personal data protection.

Cybersecurity/crime Challenges Facing the AU

- Low capacity systems that increase vulnerability
- Low technical and human capacity on IT skills
- Proliferation of cyber centers with low user regulation
- Lack of protection mechanisms at local and regional level
- Unemployment of young graduates

*The objective is **to harmonize e-legislation related to e-transactions, personal data protection, cyber security promotion, and the fight against cybercrime**,*

- Define key cyber terminology in legislation
- Develop general principles and specific provisions related to cyber legislation
- Outline cyber legislative measures required by Member States
- Develop general principles and specific provisions on international cooperation as related to cyber legislation
- Protect persons against threats and attacks that compromise their privacy during data gathering / processing
- Protecting institutions against threats and attacks capable of endangering their survival and efficacy

Legal framework-1

- **The Oliver Tambo Declaration** (Ext/CITMC/Min/Decl.(I) Johannesburg, South-Africa, 5 Nov. 2009)

  - Adoption of the resolution

- **The 14th AU Summit of Head of State and government Declaration** on "Information and Communication Technologies in Africa: Challenges and Prospects for Development" ([Assembly /AU/11(XIV)], Addis Ababa, Ethiopia, 31 January - 2 February 2010)

  - Endorsement of this resolution

- **The Abuja Declaration, CITMC-3** ([AU/CITMC/MIN/Decl.(III)], Abuja (Nigeria), 03-07 August 2010.

  - Confirmation of this resolution

We, African Ministers in charge of CIT, request the AU Commission to "Jointly finalize with the United Nations Economic Commission for Africa, within the framework of the African Information Society Initiative (AISI), the Draft Convention on Cyber Legislation and support its implementation in Member States by 2012";

Legal framework -2

- **The Khartoum Declaration** (AU/CITMC-4/MIN/Decl.(IV)Khartoum, The Sudan, 2-6 September 2012

  » Endorsement of the AU Final Draft Convention on Cyberlegislation

by the 4th Ministerial Conference of the African Union Ministers in charge of Communication and Information Technologies (CITMC-4)

II. Awareness and Capacity Building

1. Development and distribution of toolkits to facilitate the ratification of the AU Convention on Cyber security

2. Organize and participate in workshops for capacity building, awareness raising, and facilitation of national cyber security legislation in each AU member state

III. Response and Recovery Mechanisms

- ***Facilitate the setting up of National Computer Emergency Response Teams (CERTs) to contribute to the fight against cybercrime***
  - ✓ ***National CERTs***
  - ✓ ***Regional Computer Incident Response Teams (CIRTs)***
  - ✓ ***Cyber Security Unit within the AUC***

PART III: COMBATING CYBERCRIME

Section I : Terminology

Electronic communication, Computerized data, Racism and xenophobia in information and telecommunication technologies, Minor, **Child pornography**, Computer system, Exceeds authorized access, Damage …

Chapter 1: National cyber security framework

- National policy
- National strategy

Chapter 2: Legislative measures

- Legislations against cybercrime
- National Regulatory authorities
- Rights of citizens
- Protection of critical information infrastructure

www.au.int/cyberlegislation

Section II: Criminal Provisions

Chapter I: Adapting certain ICTs offenses

- Violation of property
- Criminal liability for corporate persons

Chapter II: Adapting certain sanctions to the ICTs

- Penal sanctions
- Procedural law

Chapter III: Offenses specific to ICTs

- Attack on computer systems
- Attack on computerized data
- Offenses relating to electronic message security measures.
- Content related offenses / definition of cyber threats against children

AU Member States should take necessary legislative /regulatory measures to make it a criminal offence to:

- **Produce, register, offer, manufacture, make available, disseminate and transmit an image or a representation of child pornography** through a computer system;
- **Procure** for oneself or for another person, **import** or have imported, and **export** or have exported an image or representation of child pornography through a computer system;
- **Possess** an image or representation of child pornography in a computer system **or on a computer data storage medium**;
- **Facilitate** or provide **access** to images, documents, sound or representation of a pornographic nature **to a minor**

Definitions :

Child or minor means every human being **below the age of eighteen (18)years** in the terms of the African Charter on the Rights and Welfare of the child and the UN convention on the right of the child.

Child pornography means any visual depiction, including any photograph, film, video, image, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- The production of such visual depiction involves a minor;

- Such visual depiction is a **digital image, computer image, or computer-generated image** where a minor is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge;

- **Such visual depiction has been created, adapted, or modified to appear that a minor is engaging in sexually explicit conduct.**

THANK YOU FOR YOUR ATTENTION

***

Souhila Amazouz
souhilaa@africa-union.org

AU Commission

www.au.int/cyberlegislation