

# Workshop on Harmonizing Cyberlaw in the ECOWAS region

( Procedural Law in the Budapest Convention )

Ghana, Accra

17 – 21 March 2014,

Kofi Annan International Peacekeeping Training Centre

Maureen Owor and  
Sizwe Lindelo Snail Ka Mtuze



# TABLE OF CONTENTS

Part 1: Council of Europe response to procedural aspects of cybercrime

Part 2: Concluding remarks



# Part 1: Council of Europe response to aspect of procedural law in cybercrime

## Title 2 – Expedited preservation of stored computer data

### Article 16 – Expedited preservation of stored computer data

- 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
- 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



## **Council of Europe response to aspect of procedural law in cybercrime cont.**

### **Article 17 – Expedited preservation and partial disclosure of traffic data**

- 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
  - a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
  - b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
- 2 The powers and procedures referred to in this article shall be subject to Article 14 and Article 15.



# Council of Europe response to aspects of procedural law to cybercrime cont.

## *Title 3 – Production order*

### **Article 18 – Production order**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
  - a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
  - b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
- 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
  - a the type of communication service used, the technical provisions taken thereto and the period of service;
  - b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
  - c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.



## **Council of Europe response to aspect of procedural law cybercrime cont.**

### ***Title 4 – Search and seizure of stored computer data***

#### ***Article 19 – Search and seizure of stored computer data***

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:***
  - a a computer system or part of it and computer data stored therein; and***
  - b a computer-data storage medium in which computer data may be stored in its territory.***
  
- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.***



## **Council of Europe response to procedural aspects of cybercrime cont.**

- Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- a seize or similarly secure a computer system or part of it or a computer-data storage medium;
  - b make and retain a copy of those computer data;
  - c maintain the integrity of the relevant stored computer data;
  - d render inaccessible or remove those computer data in the accessed computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



## ***Title 5 – Real-time collection of computer data***

### **Article 20 – Real-time collection of traffic data**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
  - a collect or record through the application of technical means on the territory of that Party, and
  - b compel a service provider, within its existing technical capability:
    - i to collect or record through the application of technical means on the territory of that Party; or
    - ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.





## Article 21 – Interception of content data

- 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:
  - a collect or record through the application of technical means on the territory of that Party, and
  - b compel a service provider, within its existing technical capability:
    - i to collect or record through the application of technical means on the territory of that Party, or
    - ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.
- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.



# Concluding remarks

Q & A





# Contact Us:



**Attorney : Sizwe Lindelo Snail Ka Mtuze**  
**Director - Snail Attorneys @ Law Inc.**

**E-mail : [ssnail@Snailattorneys.com](mailto:ssnail@Snailattorneys.com)**

**www : [www.snailattorneys.com](http://www.snailattorneys.com)**

**Tel / Fax : +27 (012) 362 8939**

**Fax : +27 (086) 617 5721**

**Cell : +27 (083) 477 4377**

