Workshop on effective cybercrime legislation in Eastern Africa
Dar es Salaam, Tanzania, 22 -24 August 2013

Session 5: procedural law

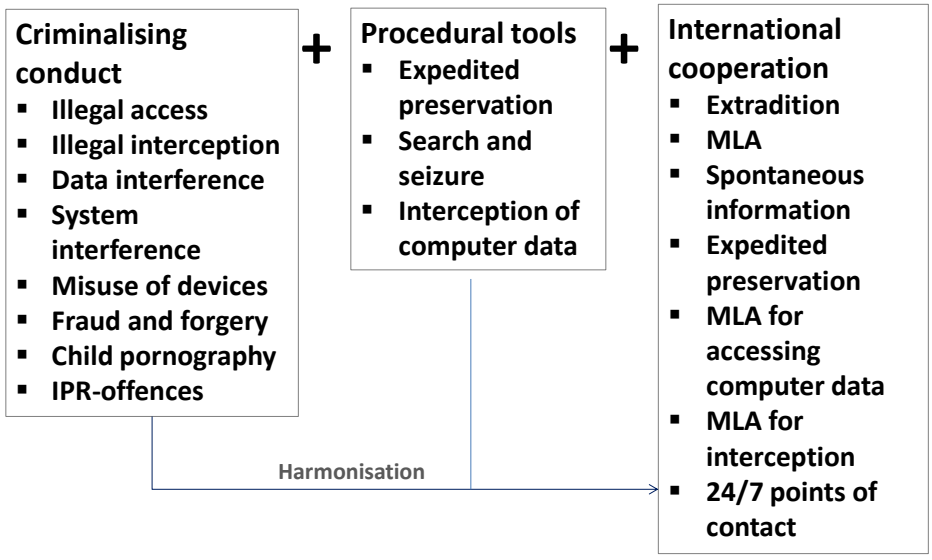
Procedural law

Alexander Seger
Secretary Cybercrime Convention Committee
Council of Europe

www.coe.int/cybercrime

1

About the scope of Budapest Convention



2

Procedural law provisions: overview

Article	Budapest Convention
Art. 15	Conditions and safeguards
Art. 16	Expedited preservation
Art. 17	Expedited preservation and partial disclosure of traffic data
Art. 18	Production order
Art. 19	Search and seizure
Art. 20	Real-time collection traffic data
Art. 21	Interception of content data
Art. 22	Jurisdiction

3

Article 16 of the Convention – 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.

4

Article 16 of the Convention – Expedited preservation of stored computer data

Uganda – CMA Section 9. Preservation Order

(1) An investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.
(2) For the purpose of subsection (1), data includes traffic data and subscriber information.
…

5

Article 16 of the Convention – Expedited preservation of stored computer data

Tanzania – Computer and Cyber Crime Bill

Section 33: Expedited preservation

If a law enforcement or police officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the law enforcement or police officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an application a judge or magistrate authorizes an extension for a further specified period of time.

6

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

7

Article 17 - Expedited preservation and partial disclosure of traffic data

Uganda CMA Section 10. Disclosure of preservation Order.

The investigative officer may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of—

(a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data; or

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or electronic key enabling access to or the interpretation of data.

8

Article 17 - Expedited preservation and partial disclosure of traffic data

Tanzania Bill Section 34 - Partial Disclosure of traffic data

If a law enforcement or police officer is satisfied computer data is reasonably required for the purposes of a criminal investigation, the law enforcement or police officer may, by written notice given to a person in control of the computer system, require the person to disclose relevant traffic data about a specified communications to identify:
the Internet service providers; and/or
the path through which a communication was transmitted.

9

Article 18 – Production order

1 ...measures to empower 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.

10

Article 18 – Production order

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

11

Article 18 – Production order

Tanzania Bill Section 32 – Production order

If a judge or magistrate is satisfied on the basis of an application by a law enforcement officer or police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the judge or magistrate may order that:

a person in the territory of United Republic of Tanzania in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or

an Internet service provider in the United Republic of Tanzania to produce information about persons who subscribe to or otherwise use the service.

12

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 Measures to ensure that where 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.

13

Article 19 - Search and seizure of stored computer data

3 Measures to empower 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 Measures to empower 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.

14

Article 19 - Search and seizure of stored computer data

Uganda Section 28. Searches and seizure.

(1) Where a Magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing—
(a) that an offence under this Act has been or is about to be committed in any premises; and
(b) that evidence that such an offence has been or is about to be committed is in those premises, the Magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary.
(2) An authorised officer may seize any computer system or take any samples or copies of applications or data—

15

Article 19 - Search and seizure of stored computer data

Tanzania Bill Section 30 – Search and seizure

(1) If a judge or magistrate is satisfied on the basis of an application by a law enforcement or police officer supported by affidavit that there are reasonable grounds or to suspect or to believe that there may be in a place a thing or computer data:
(a) that may be material as evidence in proving an offence; or
(b) that has been acquired by a person as a result of an offence;
the judge or magistrate may issue a warrant authorizing a [law enforcement or police officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access:
i) a computer system or part of it and computer data stored therein; and
ii) a computer-data storage medium in which computer data may be storedin the territory of the country.

16

Article 19 - Search and seizure of stored computer data

Tanzania Bill Section 30 – Search and seizure

(2) If a law enforcement or police officer that is undertaking a search based on Sec. 30(1) has 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, he shall be able to expeditiously extend the search or similar accessing to the other system in the territory of the country.

…..

17

Article 20 - Real-time collection of traffic data

1 measures to empower 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.

…

18

Article 20 - Real-time collection of traffic data

Tanzania Bill Section 35 - Collection of traffic data

(1) If a judge or magistrate is satisfied on the basis of an application by a law enforcement or police officer, supported by information on affidavit that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the judge or magistrate shall order a person in control of such data to:
collect or record traffic data associated with a specified communication during a specified period; or
permit and assist a specified law enforcement or police officer to collect or record that data.
….

19

Article 21 - Interception of content data

1 **Measures, 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.**

……

20

Article 21 - Interception of content data

Tanzania Bill Section 36 Interception of content data

(1) If a judge or magistrate is satisfied on the basis of an application by a law enforcement or police officer, supported by information on affidavit that there are reasonable grounds to suspect or believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the judge or magistrate may:
order an Internet service provider whose service is available in the United Republic of Tanzania through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or authorize a law enforcement or police officer to collect or record that data through application of technical means..

21

Tanzania Bill Section 37 Forensic tool

(1) If a judge or magistrate judge or magistrate is satisfied on the basis of an application by a law enforcement or police officer, supported by information on affidavit that in an investigation concerning an offence listed in paragraph 7 herein-below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part V but is reasonably required for the purposes of a criminal investigation, the judge or magistrate may authorize a law enforcement or police officer to utilize a remote forensic tool with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence.

22

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence. ……

23

Article 15 - Conditions and safeguards

1 Each Party shall ensure that ... the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

24

Article 15 - Conditions and safeguards

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

25

Article 15 - Conditions and safeguards

Rule of law requirements

In general terms, one would expect a State to meet rule of law requirements such as:

- There shall be no punishment without a law
- Everyone has the right to a fair trial, including the presumption of innocence
- Interference in the rights of individuals only in accordance with the law and as is necessary in the public interest – including crime prevention – or the protection of the rights of others. Investigative measures are to be prescribed by law
- Anyone whose rights are violated must have the right to an effective remedy
- States to put in place a framework that allows to reconcile different interests that are to be protected
- positive obligation by states to protect the rights of individuals. This may include criminal law and effective enforcement to bring offenders to justice

26

Article 15 - Conditions and safeguards

Rule of law requirements and principles with regard to procedural powers of the Budapest Convention

- **Principle of proportionality**, meaning in particular that "the power or procedure shall be proportional to the nature and circumstances of the offence". For example, particularly intrusive measures, such as interception, are to be limited to serious offences
- **Judicial or other independent supervision**
- **Grounds justifying the application of the power or procedure and the limitation on the scope or the duration**
- **Powers and procedures must be reasonable and "consider the impact on the rights, responsibilities and legitimate interests of third parties"**

27

Contact for follow up

Alexander.seger@coe.int

Secretary of the Cybercrime Convention Committee (T-CY)
Council of Europe
Strasbourg, France

www.coe.int/cybercrime

28