EU/COE Joint Project on Global Action on Cybercrime

Legislation on cybercrime and e-evidence: Procedural law

Joint ECOWAS-Council of Europe regional conference

Harmonization of legislation on Cybercrime and Electronic Evidence with rule of law and human rights safeguards

Abuja, Nigeria – 12 September 2017

Zahid Jamil
Council of Europe Expert, Pakistan

The Council of Europe Convention on Cybercrime

The approach of Council of Europe

1 Common standards: Budapest Convention on Cybercrime and related standards

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Partial disclosure of traffic data
- Production orders
- Search and seizure
- Interception of computer data

+

International cooperation

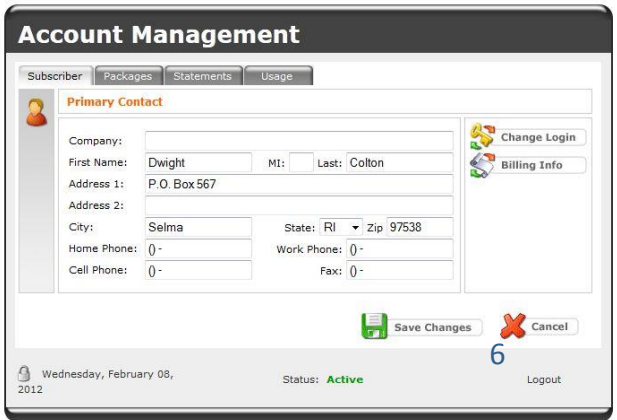
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Procedural Law

Subscriber Information

- **Information** in form of computer data/any other form held by a service provider **relating to subscribers** of its services (other than content data and traffic data)
- **Most often sought information** in criminal investigations
- **Less privacy sensitive** than traffic data and content data
- Usually **held by private sector service providers**, obtained through production orders



Subscriber Information

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.

Traffic Data

- "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Content data

- **Communication content** of the communication, i.e., the meaning or purport of the communication, or the **message or information being conveyed** by the communication (other than traffic data)
- Includes **stored content** and **future content**
- E.g. **emails, images, movies, music** and other files

Article 15 § 1
Conditions and safeguards

1. *"Each Party shall ensure that the **establishment, implementation and application** of the powers and procedures provided for in (Art. 14 to 21) are **subject to conditions and safeguards** provided for under its **domestic law** (…)".*
2. *These safeguards must "provide for the adequate protection of human rights and liberties, **including rights arising pursuant to obligations it has undertaken** under applicable international human rights instruments (inter alia the 1950 Council of Europe "European Convention of Human Rights" and the 1966 United Nations International Covenant on Civil and political Rights).*

Article 15 § 1
Conditions and safeguards

- These safeguards must “provide for the adequate protection of human rights and liberties, **including rights arising pursuant to obligations it has undertaken** under applicable international human rights instruments (inter alia the 1950 Council of Europe “European Convention of Human Rights” and the 1966 United Nations International Covenant on Civil and political Rights).
- These safeguards must incorporate “the principle of **proportionality**”.

Article 15 § 1
Conditions and safeguards

- These safeguards must “provide for the adequate protection of human rights and liberties, **including rights arising pursuant to obligations it has undertaken** under applicable international human rights instruments (inter alia the 1950 Council of Europe “European Convention of Human Rights” and the 1966 United Nations International Covenant on Civil and political Rights).
- These safeguards must incorporate “the principle of **proportionality**”.

Article 15 § 2 and 3
Conditions and safeguards

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

3. Each Party must "**consider the impact** of the powers and procedures in [Art. 14 to 21] **upon the rights**, responsibilities and legitimate interests of third parties", to the "extent that it is consistent with the public interest, in particular the sound administration of justice".

Article 15 § 2 and 3
Conditions and safeguards

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

3. Each Party must "**consider the impact** of the powers and procedures in [Art. 14 to 21] **upon the rights**, responsibilities and legitimate interests of third parties", to the "extent that it is consistent with the public interest, in particular the sound administration of justice". [1]

Conditions and safeguards under European Convention of Human Rights

Conditions to be met when limiting rights:

- Exclusive competence of the law (legal basis)
- Need to pursue a legitimate aim (**l**egitimate aim)
- “Necessity of the interference in a democratic society”... which means that the interference must:
  - correspond to a "pressing social need“ (**necessity**)
  - be proportionate to the aim pursued (**proportionality**)
- Requirements implied by the “necessity” and “proportionality” principles might be classified under the one or the other notion.

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**.*

Article 16 – Expedited Preservation of Stored Computer Data

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****.*

Article 16 – Expedited Preservation of Stored Computer Data

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**.*

Article 17 – Expedited Preservation of 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.*

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****.*

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.*

Search and Seizure of stored computer data (Article 19 – Budapest Convention)

- **Where**:
  - In a computer system or part of it
  - In a storage medium
  - In a computer system accessible from the initial one (expeditious extension of the search)
- **What**:
  - Seize or similarly secure accessed computer data
  - Power to require the necessary information to understand the functioning of the system

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*

Article 19 - Search and Seizure of Stored Computer Data

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.*

Article 19 -
Search and Seizure of Stored Computer Data

*3. 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.*

Article 19 -
Search and Seizure of Stored Computer Data

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.*

Real-time Collection of Traffic Data

(Article 20 – Budapest Convention)

- Allows alive investigations
- Intrusive measure, requires proper legislation
- Law enforcement authorities to collect or record, through technical means, data in real time, and
- Power to compel service providers to collect or record data from their costumers, in real time.

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.*

Article 20
Real-time Collection of Traffic Data

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.*

Article 20
Real-time Collection of Traffic Data

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.*

3. *The powers and procedures referred to in this article shall be **subject to Articles 14 and 15**.*

Interception of Content Data

(Article 21 – Budapest Convention)

- Very powerful investigative tool, but also very intrusive
- It is only allowed in relation to a range of serious offences to be determined by national laws
- Adequate safeguards need to be put in place

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.*

Article 21
Interception of Content Data

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.*

Article 21
Interception of Content Data

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**.*

Questions