Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

Introductory Judicial Training Course on Cybercrime and Electronic Evidence

Procedural Powers of the Budapest Convention - Part 1

JENNIFER MENSAH (MRS.)

Council of Europe

Email: jennifer.mensah@nca.org.gh

20 October 2020

Agenda

- Part One – Going Dark; The Challenge facing law enforcement
- Part Two: Procedural provisions of the Budapest Convention
- Part Three – Conditions and safeguards
- Part Four – Summary

Session Objectives

By the end of this session delegates will be able to:

- Explain the procedural provisions of the Budapest Convention.
- Explain the importance of conditions and safeguards and the way they can be determined.

How Criminals use Technology (Going Dark)

Technology as a communication tool

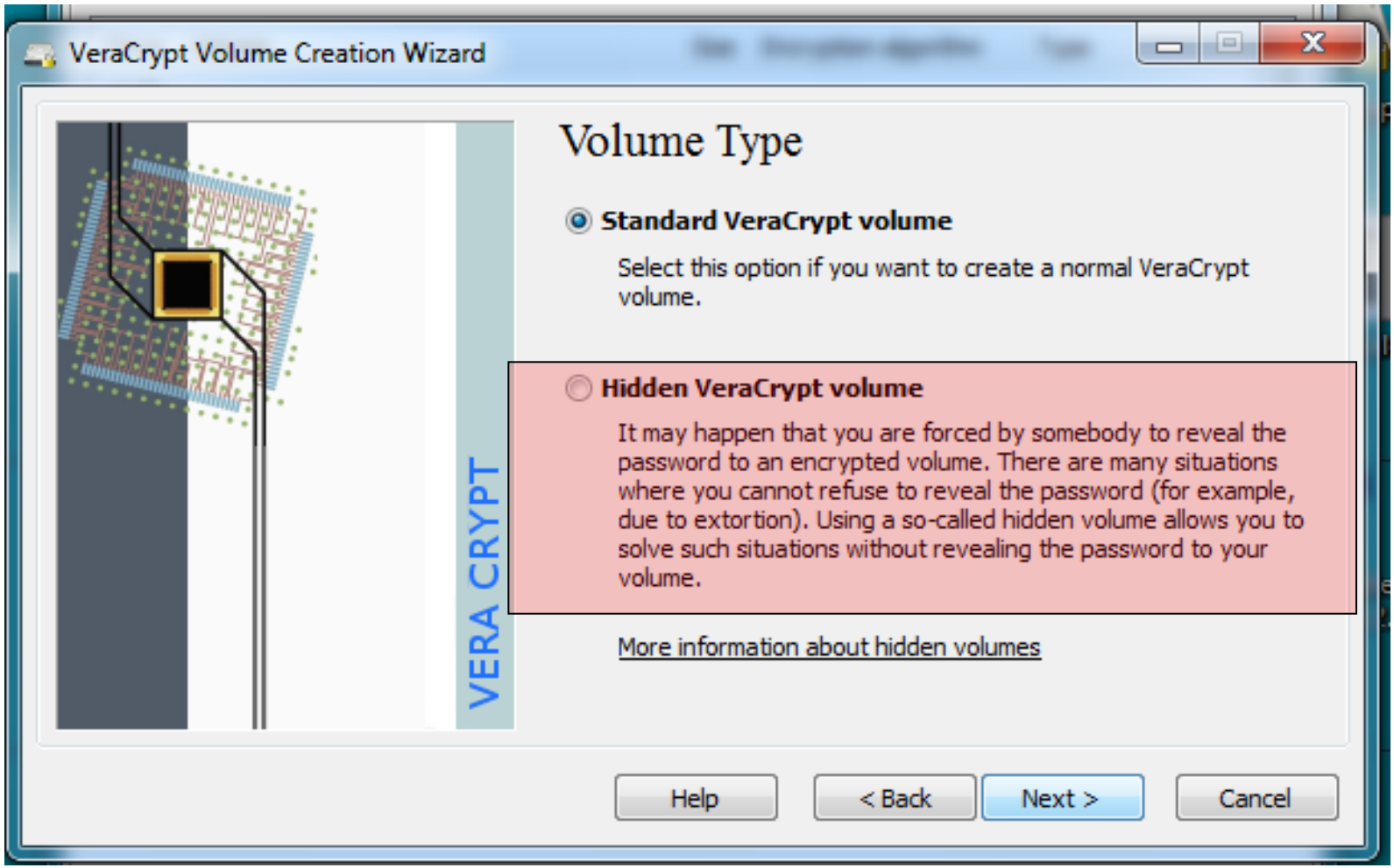
Technology as a communications tool – is where criminals use technology to communicate with each other in ways which reduce the chances of detection, for example by the use of encryption technology.

How Criminals use Technology

Technology as a storage device

Technology as a storage medium – is the intentional or unintentional storage of information on devices used in any of the other categories and typically involves the data held on computer systems of victims, witnesses or suspects.

The encryption challenge



Going Dark

- Two major encryption problems: legal intercept/wire tap (Skype/Whatsapp/Telegram) and seizure (smartphone/tablet/computer)
- The big picture today:
  no data retention, no trans-border access, too slow MLA, no direct collaboration by too many ISP's
- Possible solution : obligation to know password and give the key when requested by judge (problem of hidden containers Veracrypt)
- Punishments high enough (> 5 years)
- Let the judge decide if there is self-incrimination or not (ECHR 17 December 1996, Saunders vs. United Kingdom)

WHOIS "GOING DARK"

Challenges:

- Loss of possibility to access data promptly:

  WHOIS "going dark" – deprivation of LEA, prosecution and judiciary to promptly investigate international cybercrime;

  ICAAN results – in 2018 only 33% of WHOIS LEA requests where successful comparing to 98% before changes;

Part One
Procedural provisions of the Budapest Convention

Procedural Rules

Article 14 - scope of the procedural rules

- The rules of the Convention will be applicable
  - When the crime under investigation is one of the listed crimes in the Convention
  - In the investigation of any crime if it was committed by the means of a computer system
  - Gathering evidence in any investigation if the evidence, in the case, is kept in any kind of digital record

Articles 16 and 17

Expedited preservation of computer data and expedited preservation and disclosure of computer data

- Very innovative and extremely significant
- Different focus
  - Both of them are expedited to correspond to the speed of the circulation of information in the digital environment
  - Their intrusiveness level is not very high
  - Concerning traffic data there is also a provision allowing expedited disclosure

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

- What is the meaning of Preservation?
  - Preservation requires that data which already exists in stored form, be protected from anything that would cause its current quality or condition to change or deteriorate.
  - It does not mean legitimate users cannot use the data
  - The Convention leaves it open to countries to decide the means of preservation.
  - Perhaps a copy of the data could be used or preserved.

Article 16 – Expedited Preservation of Stored Computer Data

- What is the meaning of order or similarly obtained as specified in the article
  - This allows for the option of obtaining the data by order means and not only by Judicial or administrative orders
  - Which means Law Enforcement Agents could be granted the ability of making such preservation requests without necessarily resorting to a Judicial order.

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

- What is the importance of Article 16:
  - To preserve data that may be vulnerable to loss or modification; this includes situations where the data is subject to short retention of data period; such as a business policy may require the data be deleted within a short period of time.
  - Also to allow for the preservation of traffic data; which is usually stored by service providers for only a short period of time.
  - Allows for preservation and maintenance of the integrity of the data for a period of time up to a maximum of 90days to enable the competent authority seek its disclosure.

Article 16 – Expedited Preservation of Stored Computer Data

- What is the importance of Article 16:
  - Paragraph 3 of Article 16 imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the person ordered to preserve the data
  - So that the suspect of the investigation is not made aware of the investigation as well as the right of individuals to privacy.
  - Confidentiality is required in order that other persons do not attempt to tamper with or delete the data.

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.

Article 17 – Expedited Preservation and Partial Disclosure of Traffic Data

What is the importance of Article 17:

- Crucial Traffic data is needed to determine the source or destination of transmission of communication.
- This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service providers were involved in the transmission of specified communications.
- However, traffic data is frequently stored for only short periods of time as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore preservation measures will ensure the integrity of this data.

Article 17 – Expedited Preservation and Partial Disclosure of Traffic Data

What is the importance of Article 17:

- Competent Authorities will not know whether the service provider possesses all of the crucial traffic data or whether there were other service providers involved in the chain of transmitting the communication. Therefore this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted. In this way the investigating authorities can trace the communication back to its origin and find the perpetrators.

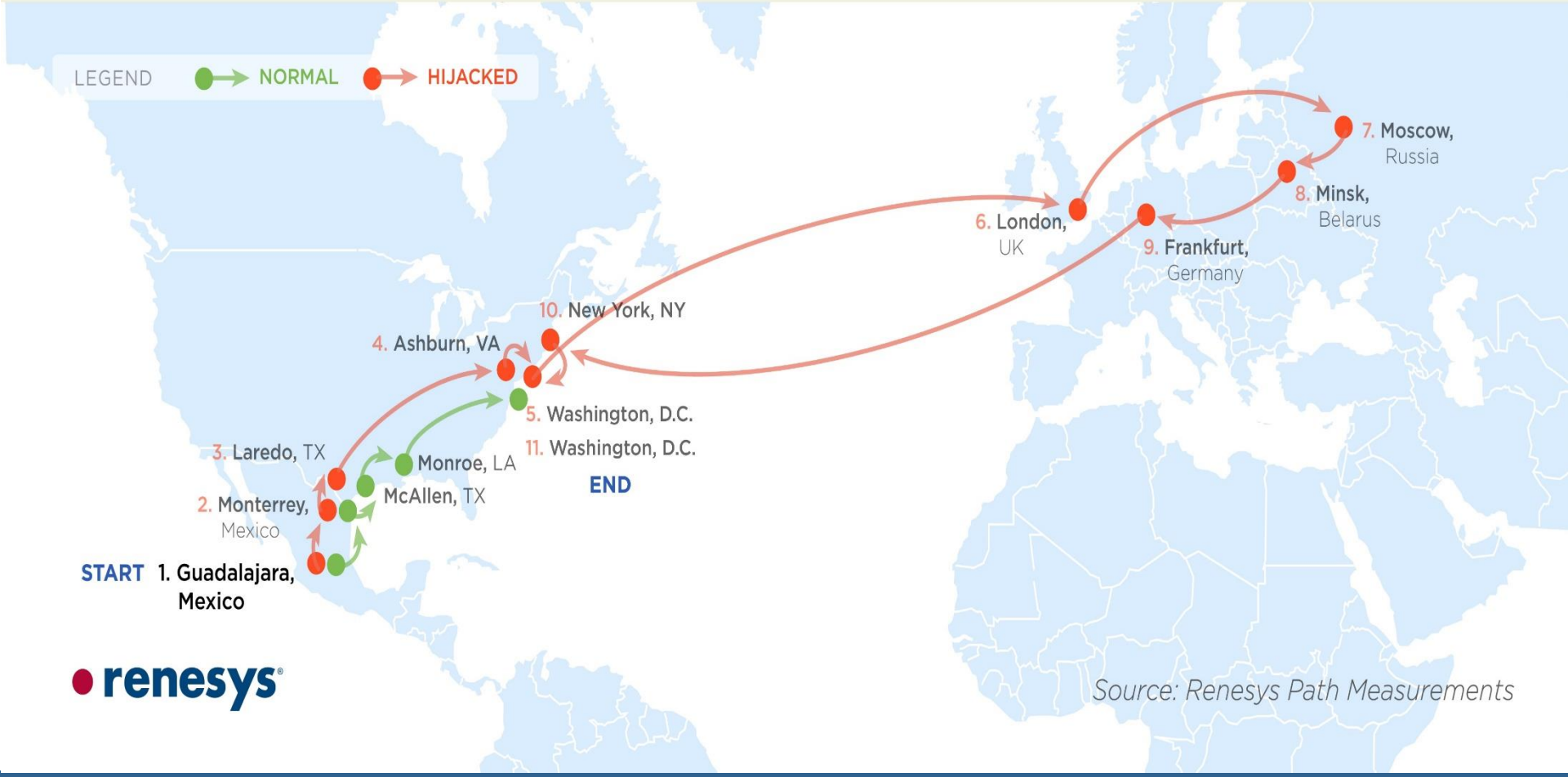
Article 17 – Expedited Preservation and Partial Disclosure of Traffic Data

What is the means of implementing Article 17?

- Competent Authorities to serve expeditiously a separate preservation order on each service provider in the communications chain.
- The preferred alternative could be to obtain a single order, the scope of which however would apply to all service providers that were identified subsequently as being involved in the transmission of the specific communication. This could be served sequentially on each service provider.
- Alternatively a service provider could notify a next service provider in the chain of the order served on it.

Expedited Preservation and Partial Disclosure of Traffic Data

Traceroute Path 1: from **Guadalajara**, Mexico to **Washington**, D.C. via ***Belarus***



Article 18

Production Orders

- Also very innovative
- To empower law enforcement authorities to issue production orders
- This order can be issued by law enforcement agencies to individuals and to Internet service providers
- Order to provide
  - data stored in a computer system under their responsibilities
  - subscriber data
- The production order must specify the nature and extent of the required data
  - the data required by the investigation must be previously determined

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.

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.

Production order

Confirmation of Yahoo fine for refusing to collaborate with Belgian police

Wednesday, 02 December 2015

The American company Yahoo has finally been charged for refusing to help the Belgian police. The firm had refused to give data to the prosecutor in Termonde. The company "provides email services in Belgium, is involved in the (local) economy, and must comply with Belgian legislation," ruled the Court of Cassation, according the daily De Standaard on Wednesday.

The facts date back to 2007 when the Termonde prosecutor asked Yahoo for information whilst investigating a case of online fraud through a Yahoo email address. The company refused to give the IP address to investigators because it said the request should be made via an international request for legal assistance. Yahoo decided American legislation applied to them. In the end, Yahoo was sentenced by the courts in Termonde in 2009. The case ended up at the Appeals Courts in Ghent, Brussels, and Antwerp, following alternating appeals by both Yahoo and the public prosecutor and judgments quashed by the Court of Cassation, which eventually confirmed the ruling by Antwerp's Appeals Court condemning Yahoo. The 44,000-euro fine for non-cooperation is therefore still applicable.

Article 19

Computer search and seizure – specific rules

- 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

Seize or similarly secure accessed computer data

- Physical seizure
- Seizure by simply making a copy of the data
- Seizure as the maintenance of the integrity of those data, keeping the data in the computer where they are stored
- Seizure, by imposing the impossibility of access to data, or even removal of specified data from a specified computer or computer 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 Seisure of Stored Computer Data

3 Each Party shall adopt such legislative and other measures as may be necessary to **empower its competent authorities to seise or similarly secure computer data** accessed according to paragraphs 1 or 2. These measures shall include the power to:

a) **seise 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.

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 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.

Procedural Powers under the Budapest Convention (Part 1)

CONDITIONS AND SAFEGUARDS

Conditions and safeguards

- 1 Each Party shall ensure that the establishment, implementation and application of 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.

- ✓ The power or procedure must be proportional to the nature and circumstances of the offence
- ✓ Domestic law must provide limitations on overbreadth of production orders and reasonableness requirements for searches and seizures.
- ✓ Parties are required to implement the principle of proportionality in accordance with domestic law

Conditions and safeguards

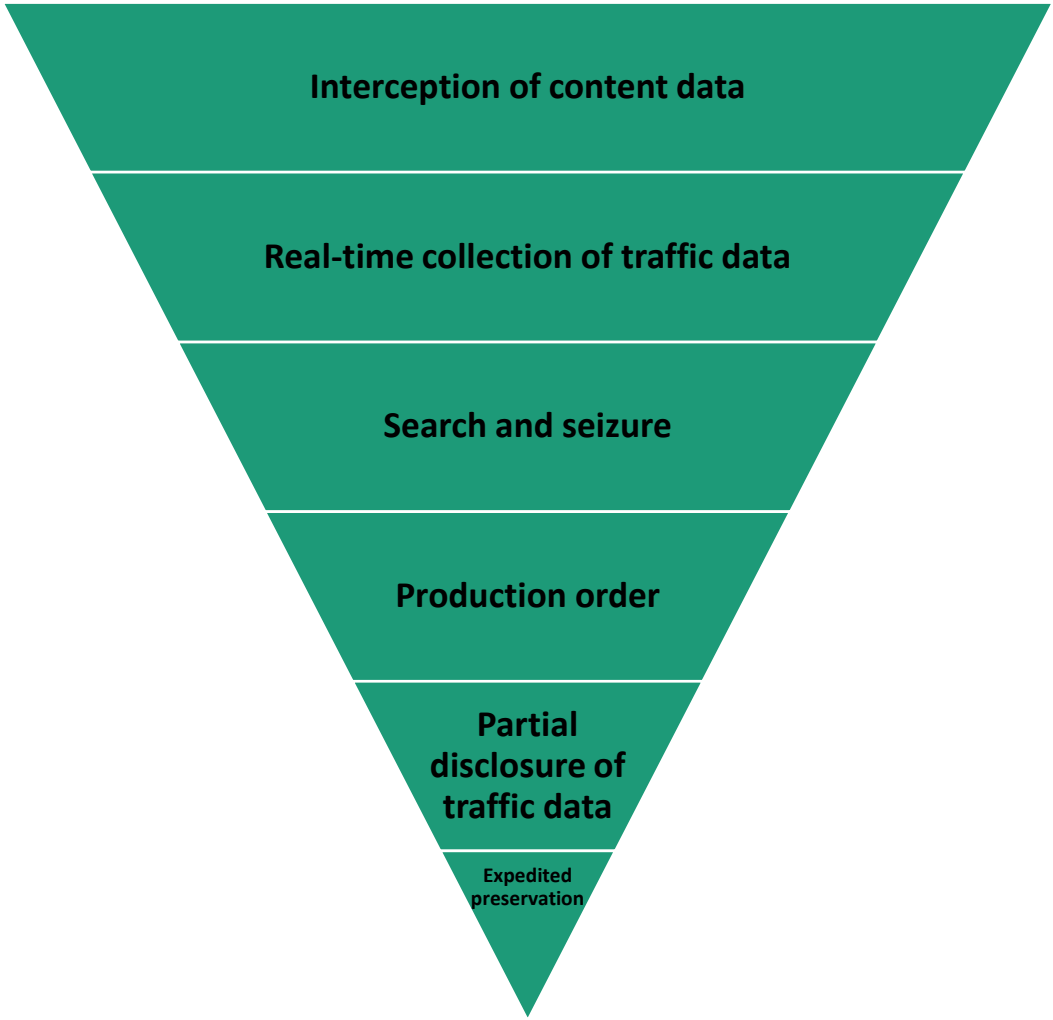
- 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including 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**.

- ✓ The power or procedure must be proportional to the nature and circumstances of the offence
- ✓ Domestic law must provide limitations on overbreadth of production orders and reasonableness requirements for searches and seizures.
- ✓ Parties are required to implement the principle of proportionality in accordance with domestic law

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.



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.

- ✓ Illustrative and non-exhaustive list of possible conditions and safeguards include:
  - ✓ Judicial supervision
  - ✓ Other independent supervision
  - ✓ Grounds justifying application of procedural powers
  - ✓ Limitation of scope of powers
  - ✓ Limitation of duration of powers

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**.

- ✓ Needs to be balanced between public interest (particularly sound administration of justice) and the rights, responsibilities and legitimate interests of third parties

- ✓ Considerations should include:
  - ✓ Minimising disruption to consumer services
  - ✓ Protection from liability for disclosure or facilitating disclosure
  - ✓ Protection of proprietary interests

Summary

By the end of this session delegates will be able to:

- Explain the procedural provisions of the Budapest Convention
- Explain the importance of conditions and safeguards and have an idea of the way they can be determined
- Explain the existing procedural provisions under the national law

Questions

Questions

References

[24] For an application of this principle at the EU level see for example a judgment of the European Union civil service tribunal (first chamber), case "V. v. European Parliament", 5 July 2011, case F-46/09, § 139, available at http://curia.europa.eu/juris/liste.jsf?language=en&num=F-46/09 (last acceded on 5 January 2017).

[25] ECtHR, case "Goodwin v. United Kingdom", Application 17488/90, 27 March 1996, §42.

[26] ECtHR, case "Klass and others v. Germany", application n° 5029/71, judgment of 6 September 1978, Series A, n° 28, §§ 50 et seq.

[27] See for example ECtHR, case of "Marckx v. Belgium", Application n° 6833/74, 13 June 1979, §31.

[28] Rec (87)15 of the Committee of ministers of the Council of Europe regulating the use of personal data in the police sector, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804e7a3c (last accessed on 5 January 2017).

[29] Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), *op. cit*., 3.26.

[30] L.H. v. Latvia (no. 52019/07) 29 April 2014; see also Kennedy v. the United Kingdom (application no. 26839/05) 18 May 2010, especially § 163.

[31] ECtHR, case "Kennedy v. the United Kingdom", 18 May 2010,

References

[32] ECtHR, case “R.E. v. the United Kingdom”, application n° 62498/11, 27 October 2015; case “Roman Zakharov v. Russia”, 4 December 2015.

[33] ECtHR, case “S & Marper v. United Kingdom”, n° 30562/04 and 30566/04, 4 Dec. 2008; E. Court H. R., case “Klass and others v. Germany”, *op. cit*., §. 55.

[34] ECtHR, case “M.G. v. the United Kingdom”, appl. n° 39393/98, *op. cit*.; E. Court H. R., case “Klass and others v. Germany”, *op. cit*., §. 56.