COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

The Convention on Cybercrime Procedural law measures

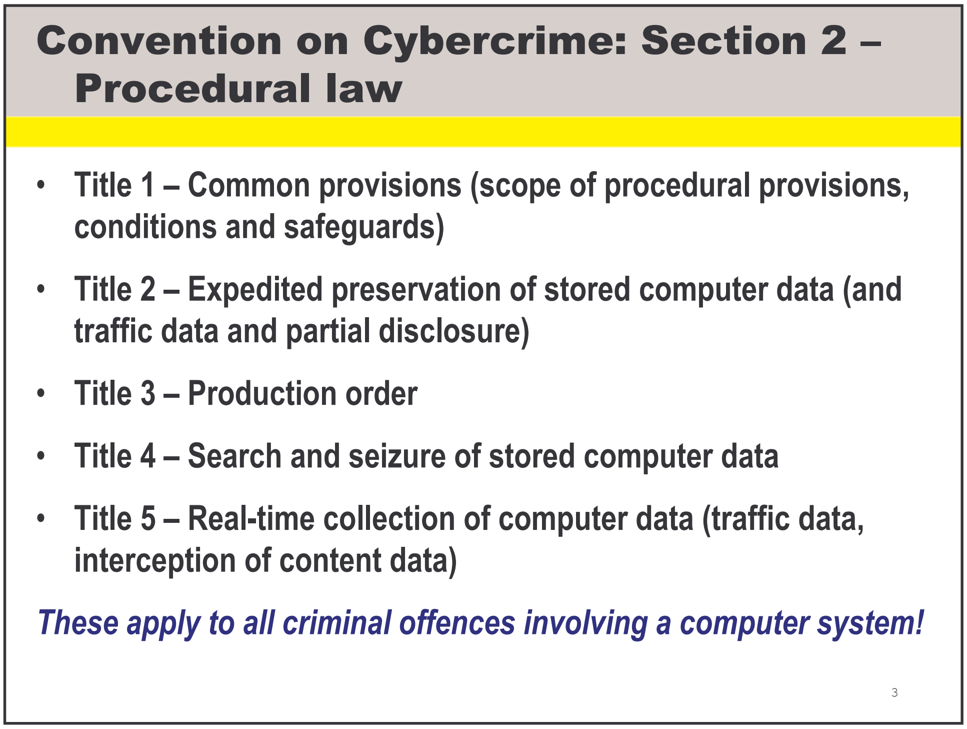
Workshop on cybercrime legislation and training of judges (Plovdiv, Bulgaria, 17-18 December 2007)

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

Procedural law

Legislation to provide for – as a minimum:

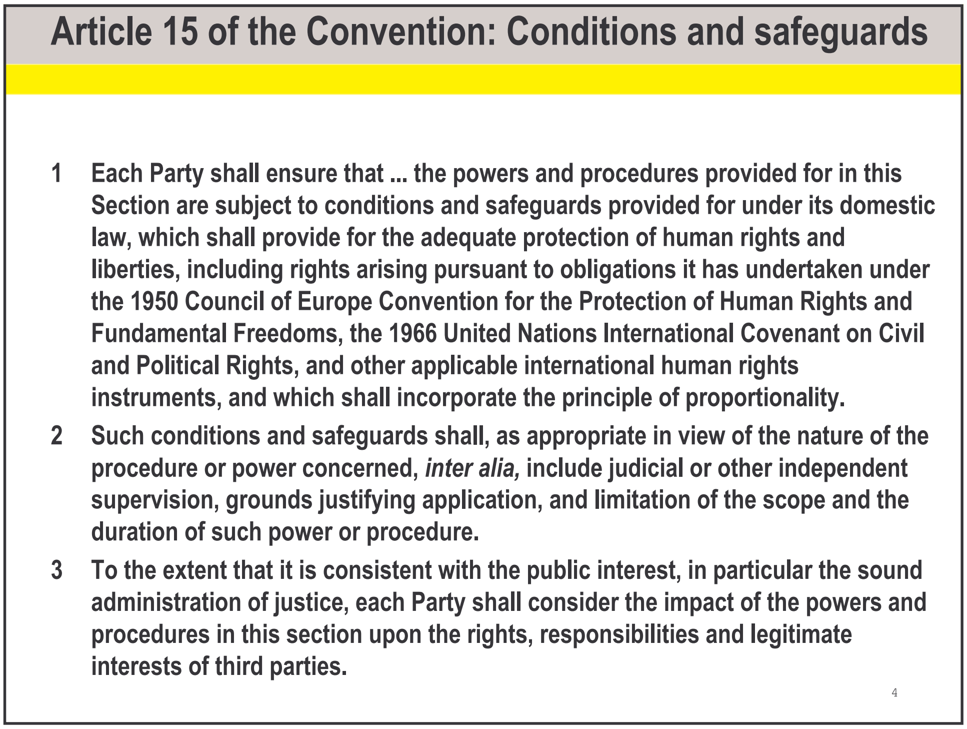
- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Procedural safeguards



Convention on Cybercrime: Section 2 – Procedural law

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
- Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)
- Title 3 – Production order
- Title 4 – Search and seizure of stored computer data
- Title 5 – Real-time collection of computer data (traffic data, interception of content data)

These apply to all criminal offences involving a computer system!



Article 15 of the Convention: 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.

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.

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.

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.

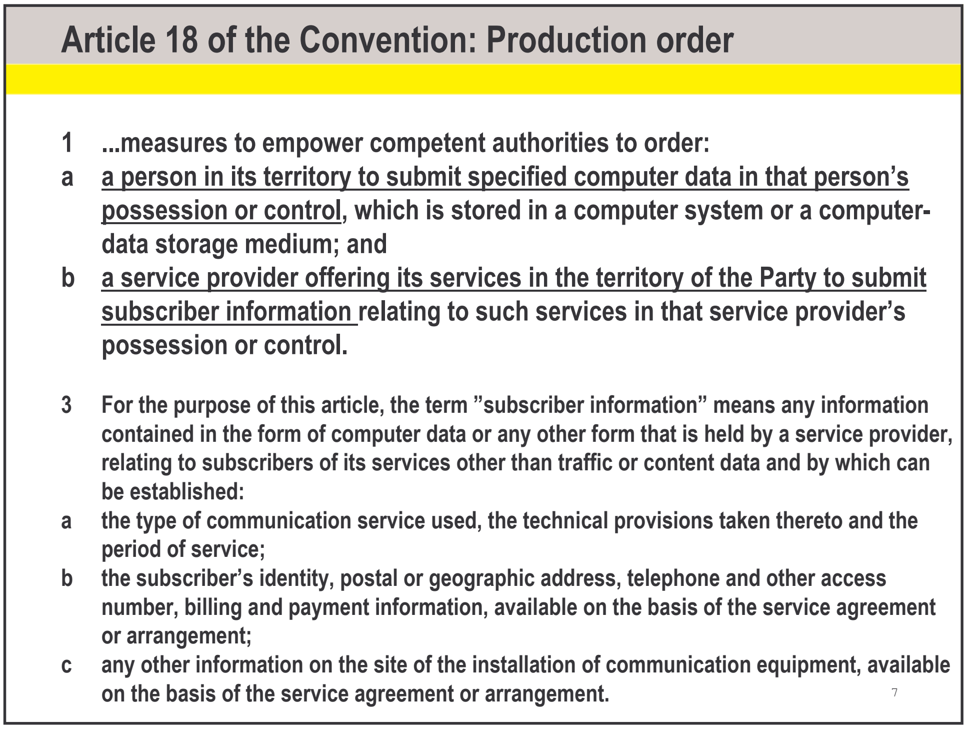
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

Article 17 of the Convention: 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 18 of the Convention: 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

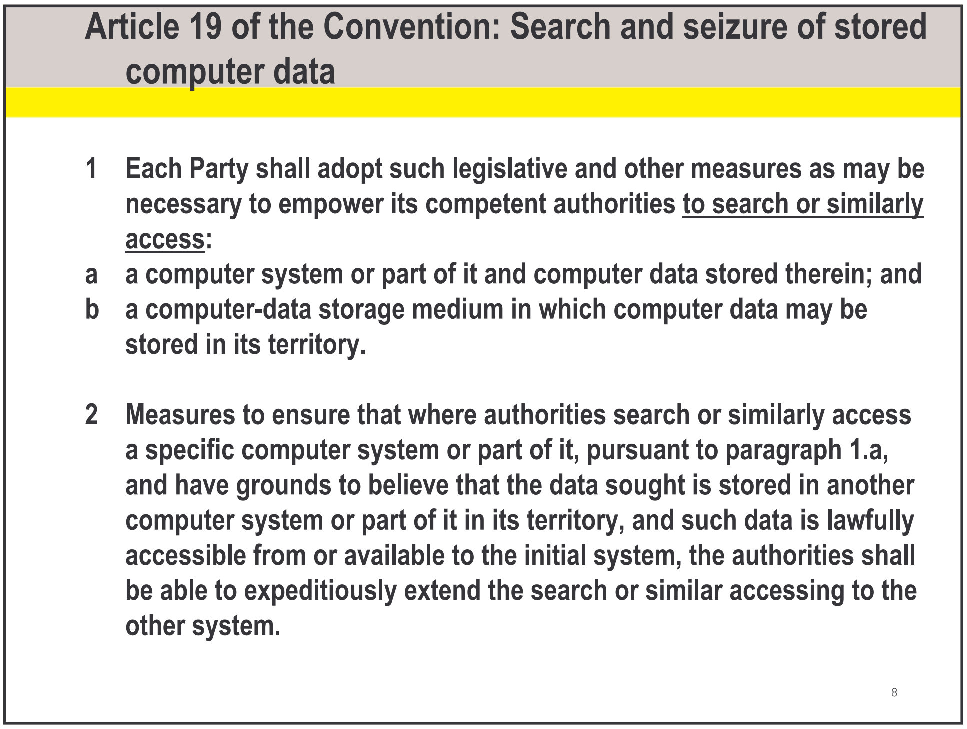
b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.

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.



Article 19 of the Convention: 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.

Article 19 of the Convention: 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.

Article 20 of the Convention: 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.

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 measures 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.

Article 21 of the Convention: 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.

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 measures 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.

Legislation and practices

Does your procedural legislation provide for:

- Expedited preservation of stored computer data?
- Expedited preservation and partial disclosure of traffic data?
- Production order?
- Search and seizure of stored computer data?
- Real-time collection of traffic data?
- Interception of content data?
- Procedural safeguards?

How does it work in practice? Case studies?

Thank you.

Alexander.seger@coe.int