

Workshop

Developing legislation on cybercrime

- **The Convention on Cybercrime as a guideline**
- **The example of Romania**

Version 1.0 (15 May 07)

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

Cristina Schulman
Ministry of Justice
Bucharest, Romania
cschulman@just.ro

Structure of the workshop

▶ Introduction

1 ▶ Defining terms

2 ▶ Substantive criminal law

3 ▶ Procedural law

4 ▶ International cooperation

➤ Provisions of the Convention

➤ Solution in Romanian legislation

➤ What solution in your legislation?

Recommended workshop materials:

- *Convention on Cybercrime and explanatory report*
- *Legislative profile for Romania*
- *Extracts from relevant national legislation*

See www.coe.int/economiccrime with a link to cybercrime

Introduction

Why legislation on cybercrime?

- **Measurable increase in cybercrimes (phishing, botnets etc)**
- **More cybercrimes for economic gain**
- **Increase in hate, racism, violence websites**
- **Software piracy**
- **Child pornography**
- **More organised cybercrime**
- **Cyberlaundering**
- **Cyberterrorism**
- **Cybercrime: low risk and many opportunities**
- **Societies around the world highly dependent on ICT and thus highly vulnerable**
- **Cybercrime is international**
- **Cybercrime is high-speed/volatile**

The legislative response

- Criminalise certain conduct ▪ **substantive criminal law**
- Give law enforcement/criminal justice the means to investigate, prosecute and adjudicate cybercrimes (immediate actions, electronic evidence) ▪ **criminal procedure law**
- Allow for efficient international cooperation ▪ harmonise legislation, provisions and institutions for **police and judicial cooperation** provisions, conclude or join agreements

The Convention on Cybercrime provides a guideline for the development of such legislation

Structure of the Convention on Cybercrime

Chapter I: Definitions

Chapter II: Measures at national level

Section 1 - Substantive criminal law

Section 2 - Procedural law

Section 3 - Jurisdiction

Chapter III: International cooperation

Section 1 - General principles

Section 2 - Specific provisions

Chapter IV: Final provisions

Defining key terms in legislation:

- **“Computer system”**
- **“Computer data”**
- **“Service provider”**
- **“Traffic data”**

Article 1 of the Convention on Cybercrime:

➤ **“computer system”** means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data

➤ **“computer data”** means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function

➤ **“service provider”** means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service

➤ **“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

The example of Romania

ART.35 (1) of Romania Law no 161/2003

➤ **“computer system”** means any device or assembly of interconnected devices or that are in an operational relation, out of which one or more provide the automatic data processing by means of a computer program

➤ **“computer data”** any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function

➤ **“service provider”** means:

i. any natural or legal person offering the users the possibility to communicate by means of a computer system;

ii. any other natural or legal person processing or storing computer data for the persons mentioned at item 1 and for the users of the services offered by these

➤ **“traffic data”** are any computer data related to a communication achieved through a computer system and its products, representing a part of the communication chain, indicating the communication origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication

Key terms:

- “Computer system”
- “Computer data”
- “Service provider”
- “Traffic data”

**How are these defined in
your legislation?**

2 Substantive Criminal Law

Legislation to deal with – as a minimum:

- **Illegal access to a computer system** (“hacking”, circumventing password protection, key-logging, exploiting software loopholes etc)
- **Illegal interception** (violating privacy of data communication)
- **Data interference** (malicious codes, viruses, trojan horses etc)
- **System interference** (hindering the lawful use of computer systems)
- **Misuse of devices** (tools to commit cyber-offences)
- **Computer-related forgery** (similar to forgery of tangible documents)
- **Computer-related fraud** (similar to real life fraud)
- **Child pornography**
- **Infringement of copyright and related rights**

Criminalising specific techniques/technologies or conduct?

Article 2 of the Convention: illegal access

➤ Establish as criminal offences under domestic law, when committed intentionally, **the access to the whole or any part of a computer system without right**. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

“Illegal access” under Romanian legislation

ART.42 of Romania Law no 161/2003

1. The access, without right, to a computer system.

A person acts without right in the following situations:

a) is not authorised, in terms of the law or a contract;

b) exceeds the limits of the authorisation;

c) has no permission from the qualified person to give it, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system.

2. The act is committed with the intent of obtaining computer data.
3. The act is committed by infringing security measures.

Article 3 of the Convention: illegal interception

- Establish as criminal offences under domestic law, when committed intentionally, **the interception without right, made by technical means, of non-public transmissions of computer data** to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

“Illegal interception” under Romanian legislation

ART.43 of Romania Law no 161/2003

- 1. The interception without right, of non-public transmissions of computer data to, from or within a computer system.**
- 2. The same penalty shall sanction the interception, without right, of electromagnetic emissions from a computer system carrying non-public computer data.**

Article 4 of the Convention: data interference

- Establish as criminal offences under domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

“Data interference” under Romanian legislation

ART.44 of Romania Law no 161/2003

- 1. Alteration, deletion or deterioration of computer data or restriction to such data without right.**
- 2. Unauthorised data transfer from a computer system.**
- 3. Unauthorised data transfer from a computer data storage medium.**

Article 5 of the Convention: system interference

- Establish as criminal offences under domestic law, when committed intentionally, the **serious hindering without right of the functioning of a computer system** by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

“System interference” under Romanian legislation

ART.45 of Romania Law no 161/2003

- **The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data**

Article 6 of the Convention: misuse of devices

- 1 Establish as criminal offences under domestic law, when committed intentionally and without right:
 - a the production, sale, procurement for use, import, distribution or otherwise making available of:
 - i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
 - ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
 - b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
- 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
- 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

“Misuse of devices” under Romanian legislation

ART.46 of Romania Law no 161/2003

1. The production, sale, import, distribution or making available, in any other form, without right, *for the purpose of committing any of the offences established in accordance with Articles 42-45, of:*
 - a) a device or a computer program designed or adapted;
 - b) a password, access code or other such computer data allowing total or partial access to a computer system.
2. The possession, without right, of a device, computer program, password, code or computer data referred to at paragraph (1) for the purpose *of committing any of the offences established in accordance with Articles 42-45.*

Article 7 of the Convention: computer-related forgery

➤ Establish as criminal offences under domestic law, when committed intentionally and without right, the **input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic**, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

“Computer-related forgery” under Romanian legislation

ART.48 of Romania Law no 161/2003

- **The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data with the intent to be used for legal purposes.**

Article 8 of the Convention: computer-related fraud

➤ Establish as criminal offences under domestic law, when committed intentionally and without right, **the causing of a loss of property to another person by:**

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

“Computer-related fraud” under Romanian legislation

ART.49 of Romania Law no 161/2003

➤ **The causing of a loss of property to another person by inputting, altering, or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another**

Article 9 of the Convention: child pornography

- 1 Establish as criminal offences when committed intentionally and without right, the following conduct:
 - a producing child pornography for the purpose of its distribution through a computer system;
 - b offering or making available child pornography through a computer system
 - c distributing or transmitting child pornography through a computer system;
 - d procuring child pornography through a computer system for oneself or for another person;
 - e possessing child pornography in a computer system or on a computer-data storage medium.

Article 9 of the Convention: child pornography

- 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
 - a a minor engaged in sexually explicit conduct;
 - b a person appearing to be a minor engaged in sexually explicit conduct;
 - c realistic images representing a minor engaged in sexually explicit conduct.
- 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
- 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

“Child pornography” under Romanian legislation

ART.51(1) of Romania Law no 161/2003

- Production of child pornography for the purpose of distribution, offering or making available, distributing or transmitting, procuring for oneself or for another person child pornography through a computer system or
- possession, without right, child pornography in a computer system or in a computer-data storage medium.

For the purpose of the present law the term “pornographic materials with minors” refer to any material presenting a minor with an explicit sexual explicit behaviour or an adult person presented as a minor with an explicit sexual explicit behaviour or images which, although they do not present a real person, simulates, in a credible way, a minor with an explicit sexual explicit behaviour.

Article 10 of the Convention: Copyright and related rights

1 Establish as criminal offences under its domestic law **the infringement of copyright**, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a **commercial scale and by means of a computer system**.

2 Establish as criminal offences under its domestic law **the infringement of related rights**, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, **on a commercial scale and by means of a computer system**.

“Infringement of copy- and related rights” under Romanian legislation

ART. 139⁸ - 139⁹ and art. 143 of Law on copyright no.8/1996

- **The act of making available to the public including through Internet or other computer networks, without the consent of the owners, the protected work or related rights or sui generis rights of the manufacturers of databases or copies of such protected work, regardless of the form of storage thereof, in such a manner as to allow to the public to access them from anywhere or at anytime individually chosen.**
- **Unauthorised reproduction of computer software in any of the following ways: install, storage, running or execution, display or intranet transmission.**
- **Distributing, importing in order to make available to the public, by digital technology, the protected work or related rights of which the information in electronic form on copyright were removed or altered without authorisation.**

How does your legislation deal with:

- **Illegal access to a computer system**
- **Illegal interception**
- **Data interference**
- **System interference**
- **Misuse of devices**
- **Computer-related forgery**
- **Computer-related fraud**
- **Child pornography**
- **Infringement of copyright and related rights by means of a computer system?**

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

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.

Expedited preservation of stored computer data under Romanian legislation

ART.54 of Romania Law no 161/2003

- In urgent and duly justified cases, if there are data or substantiated indications regarding the preparation or the committing of a criminal offence by means of computer systems, in order to gather evidence or identify the perpetrators, it can be ordered the expeditious preservation of the **computer data or traffic data**, which are subject to the danger of destruction or alteration.
- The preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
- The measure is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
- The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data, the respective person being obliged to expeditiously preserve them under confidentiality conditions.

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

Expedited preservation and partial disclosure of traffic data under Romanian legislation

ART.54 of Romania Law no 161/2003

- **Expedited preservation of computer and traffic data (see above)**
- **In case the data referring to the traffic data is under the possession of several service providers, the service provider is bound to immediately make available for the criminal investigation body the information necessary to identify the other service providers in order to know all the elements in the communication chain used.**

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.

Production order under Romanian legislation

ART. 16 of Law no 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences

- **The public prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may order any person who holds or from whom emerge to communicate the originals or copies of any data, information, documents, banking, financial or accounting documents and other such items, and such person shall be bound to comply.**
- **Failure to observe the obligation in paragraph (2) shall entail judicial liability, under the law.**
- **For the purpose of the present law: “*data on the users*” means any information that can lead to identifying a user, including the type of communication and the serviced used, the post address, geographic address, IP address, telephone numbers or any other access numbers and the payment means for the respective service as well as any other data that can lead to identifying the user**

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.

Search and seizure of stored computer data under Romanian legislation

For art. 19 (3) of Convention on Cybercrime - ART. 96 and Art.99 of Criminal procedure Code. For art.19 (1-2) of Convention on Cybercrime - ART.56 (1) (3) of Romania Law no 161/2003.

- Whenever for the purpose of discovering or gathering evidence it is necessary to investigate a computer system or a computer data storage medium, the prosecutor or court can order a search.
- When, on the occasion of investigating a computer system or a computer data storage medium it is found out that the computer data searched for are included on another computer system or another computer data storage medium and are accessible from the initial system or medium, it can be ordered immediately to authorize performing the search in order to investigate all the computer systems or computer data storage medium searched for.

Criminal procedure Code

ART. 96 - Confiscation of objects and writings

ART. 99 - Confiscation by force of objects or writings

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.

Real-time collection of traffic data under Romanian legislation

ART.54 of Romania Law no 161/2003

- **The provision for the preservation of computer data or traffic data is also used for the real-time collection of traffic data**

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**.

Interception of content data under Romanian legislation

ART.57 of Romania Law no 161/2003

- **The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when useful to find the truth and the facts or identification of the perpetrators cannot be achieved on the basis of other evidence**

How 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?

4 International Cooperation

Chapter III of the Convention - International cooperation

Section 1 – General principles

- **Art 23 General principles on international cooperation**
- **Art 24 Principles related to extradition**
- **Art 25 Principles related to mutual legal assistance**
- **Art 26 Spontaneous information**
- **Art 27 MLA in the absence of applicable international instruments**
- **Art 28 Confidentiality and limitation on use**

Chapter III - International cooperation

Section 2 – Specific provisions

- **Art 29 - Expedited preservation of stored computer data**
- **Art 30 - Expedited disclosure of preserved computer data**
- **Art 31 - Mutual assistance regarding accessing stored computer data**
- **Art 32 - Trans-border access to stored computer data (public/with consent)**
- **Art 33 - Mutual assistance in real-time collection of traffic data**
- **Art 34 - Mutual assistance regarding interception of content data**
- **Art 35 - 24/7 network**

How does your legislation cover:

- **General principles on international cooperation**
- **Extradition**
- **Principles related to mutual legal assistance**
- **Spontaneous information**
- **MLA in the absence of applicable international instruments**
- **Confidentiality and limitation on use**

How does your legislation provide for:

- Expedited preservation of stored computer data
- Expedited disclosure of preserved computer data
- Mutual assistance regarding accessing stored computer data
- Trans-border access to stored computer data (public/with consent)
- Mutual assistance in real-time collection of traffic data
- Mutual assistance regarding interception of content data
- 24/7 network