www.coe.int/cybercrime

Council of Europe Convention on cybercrime and national implementation

Cristina Schulman
Council of Europe
Strasbourg, France
Tel +33-3-8841-2103
cristina.schulman@coe.int

Convention on Cybercrime: Structure

- 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

ROMANIA example

Title III of the Law 161/2003 on preventing and fighting cybercrime

- Chapter I - General Provisions (definitions)
- Chapter II - Prevention of cybercrime
- Chapter III - Crimes and contraventions
- Chapter IV - Procedural provisions
- Chapter V - International Cooperation

Article 1 of the Convention – Definitions

For the purposes of this Convention:

a. **"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;

b. **"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;

c. **"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;

d. **"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.

Romanian law on cybercrime: definitions

Art. 35 Law no 161/2003

- *computer system*
- *computer data*
- *service provider*
- *traffic data*
- *child pornography*
- *data on the users (subscriber information)*

- *automatic data processing*
- *computer program*
- *security measures*
- *without right*

The term: ''without right'' - Article 35 (2) of Law no 161/2003
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.

The intentional element -Article 19 paragraphs 2-3 of the Criminal Code
(2) An act that resides in an action committed with negligence shall be an offence only when the law provides this expressly.

Convention on Cybercrime: Substantive law

Chapter II – Measures at national level
Section 1 – Substantive criminal law

Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems:

- illegal access
- illegal interception
- data interference
- system interference
- misuse of devices

Title 2 – Computer-related offences:

- Computer - related forgery
- Computer - related fraud

Title 3 – Content-related offences (child pornography)

Title 4 – Infringements of copyright and related rights

Title 5 – Ancillary liability and sanctions (attempt and aiding or abetting, corporate liability, sanctions and measures)

Illegal access

CONVENTION	ROMANIA
Article 2 - Illegal access ➢access to the whole or any part of a computer system without right ▪ ***infringing security measures*** ▪ ***with the intent of obtaining computer data or other dishonest intent*** ▪ ***in relation to a computer system that is connected to another***	**Article 42 - Law on cybercrime** (1) The **access without right to a computer system** is a criminal offence and is punished with imprisonment from 6 months to 3 years or a fine. (2) Where the act provided in paragraph (1) is committed with the **intent of obtaining computer data** the punishment is imprisonment from 6 months to 5 years. (3) Where the act provided in paragraphs 1-2 is committed by **infringing the security measures**, the punishment is imprisonment from 3 to 12 years.

ROMANIA (Art. 42 - Law on cybercrime)

Illegal access

(2) Where the act provided in paragraph (1) is committed with **the intent of obtaining computer data** the punishment is imprisonment from 6 months to 5 years.

ROMANIA (Art. 44 - Law on cybercrime)

Data interference

(2) The **unauthorised data transfer from a computer system** is punished with imprisonment from 3 to 12 years.
(3) The same punishment as in paragraph (2) shall sanction the **unauthorised data transfer by means of a computer data storage medium.**

Illegal interception

CONVENTION	ROMANIA
Article 3 - Illegal interception **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.** ▪ ***committed with dishonest intent, or in relation to a computer system that is connected to another computer system.***	**Article 43 - Law on cybercrime** (1) The **interception without right of non-public transmissions of computer data** to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years. (2) The same punishment shall sanction the **interception, without right, of electromagnetic emissions** from a computer system carrying non-public computer data.

Data interference and system interference

CONVENTION	ROMANIA
Article 4 - Data interference **The damaging, deletion, deterioration, alteration or suppression of computer data without right.** ***result in serious harm.***	**Article 44** - **Law on cybercrime** (1) The **alteration, deletion or deterioration of computer data or restriction to such data** without right is a criminal offence and is punished with imprisonment from 2 to 7 years. (2) The unauthorised data transfer from a computer system is punished with imprisonment from 3 to 12 years. (3) The same punishment as in paragraph (2) shall sanction the unauthorised data transfer by means of a computer data storage medium.
Article 5 – System interference **The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.**	**Article 45 - Law on cybercrime** 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 is a criminal offence and is punished with imprisonment from **3 to 15 years.**

Misuse of devices

CONVENTION	ROMANIA
Article 6 - Misuse of devices **The production, sale, procurement for use, import, distribution or otherwise making available of:** **-a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in Articles 2 through 5** **- 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 the intend to be used …** **- the possession**	**Article 46 - Law on cybercrime** (1) It is a criminal offence and shall be punished with imprisonment from 1 to 6 years. a)the **production, sale, import, distribution or making available, in any other form**, without right, of a device or a computer program designed or adapted for the purpose of committing any of the offences established in accordance with Articles 42-45; b)the **production, sale, import, distribution or making available, in any other form,** without right, of a password, access code or other such computer data allowing total or partial access to a computer system **for the purpose of committing any of the offences established in accordance with Articles 42 - 45;** 2) The same penalty shall sanction the **possession**, without right, of a device, computer program, password, access 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.**

Computer – related offences

CONVENTION	ROMANIA
Article 7 - Computer - related forgery **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.** ***an intent to defraud, or similar dishonest intent, before criminal liability attaches.***	**Article 48 - Law on cybercrime** 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**, is a criminal offence and shall be punished with imprisonment from 2 to 7 years.
Article 8 – Computer related fraud **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.**	**Article 49 - Law on cybercrime** 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 anothe**r shall be punished with imprisonment from 3 to12 years.

Child pornography

CONVETION	ROMANIA
Article 9 **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** **Define: "child pornography" and ''minor''**	**Article 51 - Law on cybercrime** (1) It is a criminal offence and shall be punished with imprisonment from 3 to 12 years and denial of certain rights the **production for the purpose of distribution**, **offering or making available**, **distributing or transmitting**, **procuring for oneself or another of child pornography material** through a computer system, or **possession,** without right, child pornography material in a computer system or computer data storage medium. **Art. 35 (1)** i) ***„pornographic materials with minors"*** refer to any material presenting a minor with an explicit sexual behaviour or an adult person presented as a minor with an explicit sexual behaviour or images which, although they do not present a real person, simulates, in a credible way, a minor with an explicit sexual behaviour.

Infringements of copyright and related rights

CONVENTION	ROMANIA
Article 10 - Infringements of copyright and related rights **- the law of that Party (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)** **law of that Party (the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty)** ***committed wilfully, on a commercial scale and by means of a computer system.***	**Law on copyright (No. 8/1996) (amended)** ▪ **making available to the public including by Internet or other computer networks** the protected work ▪ 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 of which the information in electronic form on copyright or related rights were removed or altered without authorisation.

CONVENTION

Article 11 – Attempt and aiding or abetting

Article 12 – Corporate liability

CONVENTION	ROMANIA
Article 13 – Sanctions and measures	Art. 42 – 49, 51 Law on cybercrime Art. 53[1] Criminal Code Law 8/1996 (amended) illegal access: 6 months - 12 years (with qualified versions) illegal interception: 2 - 7 years data interference: 2 - 12 years (with qualified versions) system interference: 3 - 15 years misuse of device: 1 - 6 years computer related forgery: 2 - 7 years computer related fraud: 3 - 12 years child pornography: 3 - 12 years Infringements of copyright and related rights: 3 months – 4 years or a fine Criminal liability of legal persons - fine from 2.500 - 2.000.000 RON /complementary penalties (ART. 53[1] Criminal Code)

CONVENTION	ROMANIA Law on cybercrime: possible gaps
Article 2 - Illegal access access to the whole or any part of a computer system without right	access without right to a computer system
Article 3 - Illegal interception interception without right, made by technical means, of non-public transmissions	interception without right of non-public transmissions
Article 6 - Misuse of devices the production, sale, procurement for use, import, distribution or otherwise making available	the production, sale, import, distribution or making available, in any other form
Article 7 - Computer - related forgery regardless whether or not the data is directly readable and intelligible (inauthentic data)	?
Article 10 - Infringements of copyright and related rights where such acts are committed wilfully, on a commercial scale and by means of a computer system	?
Article 12 – Corporate liability	some requirements missing

Convention on Cybercrime: Procedural law

Minimum standards under Convention

- 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
- Conditions and safeguards

- Scope of procedural provisions: apply to:
  - *criminal offences provided by Art. 2 - 11 of the Convention;*
  - *other criminal offences committed by means of a computer system; and*
  - *collection of evidence in electronic form of a criminal offence*

Scope of procedural provisions

CONVENTION	ROMANIA
Article 14 – Scope of procedural provisions **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*** **.**	**Article 58 - Law on cybercrime** The provisions of this chapter are applicable to criminal investigations or during the trial for the offences stipulated in this title or **any other offences committed by means of computer systems.**

Conditions and safeguards

CONVENTION	ROMANIA
Article 15 – Conditions and safeguards adequate protection of human rights and liberties (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)	ART. 26 (1) 27 (3), 28 of Constitution of Romania ART. 91^1 Criminal procedure Code ART. 57 (1) (2) of Law no. 161/2003 on cybercrime ART. 3 (3) (5) of Law no. 365/2002 on electronic commerce (amended by Law no 121/2006)

Expedited preservation of stored computer data

CONVENTION	ROMANIA
Article 16 – Expedited preservation of stored computer data 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. - to **oblige a 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 **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	**Article 54 - Law on cybercrime** In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation or the committing of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying 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** or during the trial by the **court order** The measure - over a period no longer than 90 days (can be exceeded for 30 days). The prosecutor's ordinance or the court order is sent, immediately, **to any service provider or any other person possessing the data** referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.

Expedited preservation and partial disclosure of traffic data

CONVENTION	ROMANIA
Article 17 – Expedited preservation and partial disclosure of traffic data 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 reservation 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	**Art. 54 (5) - Law on cybercrime** 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. Until the end of the criminal investigation, the prosecutor is obliged to **advise, in writing, the persons** that are under criminal investigation and the data of whom were preserved.

Production order

CONVENTION	ROMANIA
Article 18 – Production order 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.	**Law no. 508/2004 on establishing, organizing and operating of the DIOCTO** The prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may order to obtain in original or copy, **any data, information, documents, banking, financial or accounting documents and other such items,** by **any person who holds them or from whom they emerge**, and such person shall be bound to comply. Failure to observe the obligation in paragraph (2) shall entail legal liability, under the law. g*) "**data on the users"*** are represented by 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;

CONVENTION	ROMANIA : Law on cybercrime: Art. 55, 56, 59
Article 19 – Search and seizure of stored computer data	The prosecutor, on the basis of the motivated authorisation …or the court **orders on the seizing of the objects containing computer data, traffic data or data regarding the users**, from the person or service provider possessing them, in view of making copies that can serve as evidence. If the objects containing computer data or traffic data are not given willingly to the judicial authorities in order to make copies, the prosecutor mentioned in paragraph (1) or **court orders the forced seizure** 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.** If the criminal investigation body or the court considers that seizing the objects that contain the data referred to at paragraph (1) would severely affect the activities performed by the persons possessing these objects, it can **order performing copies that would serve as evidence …** 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.** ▪ for the criminal offences stipulated in this law and any criminal offences committed by means of computer systems, in order to ensure the **special seizure** stipulated at art.118 of the Criminal Code it can be performed the prevention measures provided for by the Criminal Procedure Code. ▪**Criminal procedure Code: ART. 96 - Confiscation of objects and writings ; ART. 99 - Confiscation by force of objects or writings**

Real-time collection of traffic data

Real-time collection of traffic data	ROMANIA
Article 20 – Real-time collection of traffic data **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.**	**Considered under the new Criminal Procedure Code**

Interception of content data

CONVENTION	ROMANIA
Article 21 – Interception of content data 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.	**Art. 57 - Law on cybercrime** 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. **Article 91^1 (Section V^1) of the Criminal Procedure Code on audio and video interception and recording of conversations or communications by telephone or by any other electronic means of communication**

CONVENTION	ROMANIA Law - possible gaps
Article 16 – Expedited preservation of stored computer data expeditious preservation of specified computer data, including traffic data	preservation of the computer data or the data referring to data traffic
Article 17 – Expedited preservation and partial disclosure of traffic data a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted	the information necessary to identify the other service providers in order to know all the elements in the communication chain used
Article 20 – Real-time collection of traffic data	?
Article 18 – Production order	general provisions

Convention on Cybercrime: a framework for international cooperation

The Convention aims:

- Harmonize the domestic criminal substantive law elements of offences and related provisions in the area of cybercrime

- Provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system

- **Establish a fast and effective framework for 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

Mutual Legal Assistance

Art 25 - MLA - subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation

Art 27 - MLA in the absence of applicable international instruments provides a minimum set of rules in the absence of an MLAT or other arrangements: establish central authorities, procedures in cases of postponement or refusal of the request, confidentiality of requests, and direct communications

Europe: Applicable instruments on judicial cooperation :

- European Convention on Mutual Legal Assistance in Criminal Matters, Strasbourg, 20.04.1959
- Additional Protocol to the European Convention on Mutual Assistance in Criminal, Strasbourg, 17.03.1978
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 8.11.2001
- Romania applies the Convention in relation with non EU countries or EU countries that are not parties to the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (Grece, Italy, Ireland, Luxemburg)
- United Nations Convention against Transnational Organized Crime, 2000 New York (*offences involving an organized criminal group)*
- Other multilateral/bilateral treaties

International cooperation

Law no. 302/2004 on international judicial cooperation in criminal matters (amended by the Law No. 224/2006)

This law applies to the following forms of international judicial co-operation in criminal matters:

- extradition;
- surrender based on a European Arrest Warrant;
- transfer of proceedings in criminal matters;
- recognition and enforcement of judgements;
- transfer of sentenced persons;
- judicial assistance in criminal matters;
- other forms of international judicial co-operation in criminal matters.

Constitution of ROMANIA - Article 11:

(1) The Romanian State pledges to fulfil as such and in good faith its obligations as deriving from the treaties it is a party to.

(2) Treaties ratified by Parliament, according to the law, <u>are part of national law.</u>

Title III of the Law 161/2003 on preventing and fighting cybercrime (Chapter V - International Cooperation (Articles 60 – 66)

Romanian legal authorities cooperate directly, under the conditions of the law and by **observing the obligations resulting from the international legal instruments of which Romania is Party of,** with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.

Scope of cooperation:

- international legal assistance in criminal matters
- extradition
- identification, blocking, seizing or confiscation of the products and instruments of the criminal offence
- carrying out common investigations
- exchange of information
- technical assistance or of any other nature for the collection of information
- specialised personnel training
- other such activities

MLA examples: service of documents in cases related to computer-related fraud

1. The service of documents has been solicited to the following states:

- USA, Canada, Brazil, Ireland and the Dominican Republic: 122 victims in US, Ireland (1), Brazil (1), Canada (1), the Dominican Republic (1).

- no bilateral treaty with the Dominican Republic (the request had to be transmitted through diplomatic channels and unfortunately to another South-American Country where Romania had diplomatic representatives.

- only one response was received, from Ireland

According to the national law if only one proof of service does not return for the specified date, the court has to set another term for the trial

2. 26 victims in Romania (1), US (18), Netherlands (1), Canada (4), China (2).

Due to the fact that the proof of service of some of the summoning documents never returned, the court was forced to adjourn the case several times, the terms granted being of 6, 7 months each time. This caused a remarkable delay.

Some cases are pending for years.

International cooperation under existing MLA agreements. Need to be improved?

The fight against cybercrime requires increased, rapid, and well-function international cooperation in criminal matters

Effective combating of crimes committed by means of a computer system and effective collection of evidence in electronic form require a very rapid response

Mutual assistance regarding provisional measures or regarding investigative powers might be essential for an investigation

In most cases investigated the Romanian authorities send at least a request for information to foreign authorities using any of the accepted police channels but the reply time even for information exceeds 20-30 days.

Pre-trial investigation and than the trial take a long time, given the procedure for summoning persons who live abroad (the summoning is executing according to MLA treaties concluded by Romania).

Directorate for Investigating Organized Crime and Terrorism Offences

Difficulties in dealing with cybercrime arise from the extraneous element which is present in 80% of the cases.
It has to be distinguished between:
• offences committed in Romania but the results of which occur abroad;
• offences committed both in Romania and abroad committed by Romanian nationals but also foreign nationals;
• offences committed entirely outside Romania but the proceeds of the offence are collected in Romania.
These led to a delay in assessing the evidence in order to be included in the indictments or administrate them before courts.

Chapter III – International co-operation
Section 2 - Specific provisions

- Art. 29 - Expedited preservation of stored computer data
- Art. 30 - Expedited disclosure of preserved traffic data
- Art.31 - Mutual assistance regarding accessing of stored computer data
- Art. 32 -Trans-border access to stored computer data with consent or where publicly available
- Art. 33 - Mutual assistance in the real-time collection of traffic data
- Art. 34 - Mutual assistance regarding the interception of content data

Expedited preservation of stored computer data

CONVENTION	ROMANIA
Article 29 – Expedited preservation of stored computer data ➢a Party requests for the expeditious preservation of data stored in the territory of the requested Party by means of a computer system. ➢ contents of a request; ➢ the principle that dual criminality shall not be required; ➢ reserve the right to refuse to preserve where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be met; ➢ grounds for refusal; ➢ held for at least 60 days	**Article 63 - Law on cybercrime** Within the international cooperation, the competent foreign authorities can **require from the Service for combating cybercrime the expeditious preservation of the computer data or of the data regarding the traffic data existing** within a computer system on the territory of Romania, related to which the foreign authority is to formulate a request of international legal assistance in criminal matters. The preservation request is executed according to art. 54 for a period of **60 days at the least** and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters;

Expedited disclosure of preserved traffic data

CONVENTION	ROMANIA
Article 30 – Expedited disclosure of preserved traffic data ▪a service provider in another State was involved in the transmission of the communication ▪ disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted ▪ grounds for refusal	**Article 64 - Law on cybercrime** If, in executing the request for the expeditious preservation a service provider in another state is found to be in possession of the data regarding the traffic data, the Service for combating Cybercrime Fighting Service will immediately inform the requesting foreign authority about this, communicating also **all the necessary information for the identification of the that service provider**

Article 31 - Mutual assistance regarding accessing of stored computer data

- request to **search or similarly access, seize or similarly secure, and disclose data** stored by means of a computer system, including data that has been preserved pursuant to Article 29
- terms and conditions for providing such co-operation should be those set forth in applicable treaties, arrangements and domestic laws governing mutual legal assistance in criminal matters
- on an **expedited basis** where

  (1) there are grounds to believe that relevant data is particularly vulnerable to loss or modification, or

  (2) otherwise where such treaties, arrangements or laws so provide

Article 32 –Trans-border access to stored computer data

- A Party may, without the authorisation of another Party:

  a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

  b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system

CONVENTION	ROMANIA
Article 32 – Trans-border access to stored computer data with consent or where publicly available	**Article 65 - Law on cybercrime** A competent foreign authority can have access to **public Romanian sources of computer data <u>without requesting the Romanian authorities</u>**. A competent foreign authority can have access and can receive, by means of a computer system located on its territory**, computer data stored in Romania, if it has the approval of the authorised person, under the conditions of the law,** to make them available by means of that computer system, without requesting the Romanian authorities.

Article 33 –Mutual assistance in the real-time collection of traffic data

- each Party is under the obligation to collect traffic data in real time for another Party
- the terms and conditions by which such co-operation is to be provided are set forth in applicable treaties, arrangements and laws governing mutual legal assistance in criminal matters
- assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case

Article 34 – Mutual assistance regarding the interception of content data

- provide mutual assistance in the real-time collection or recording of content data of specified communications transmitted by means of a computer system
- to the extent permitted under their applicable treaties and domestic laws

CONVENTION	ROMANIA
Articles 31, 33-34 Mutual assistance regarding: ▪accessing of stored computer data ▪real-time collection of traffic data ▪ interception of content data	Article 60- Law on cybercrime The Romanian legal authorities cooperate with the institutions having similar attributions from other states and the international organisations specialised Scope of cooperation: ▪international legal assistance in criminal matters ▪extradition ▪identification, blocking, seizing or confiscation of the products and instruments of the criminal offence ▪carrying out common investigations ▪exchange of information ▪technical assistance or of any other nature for the collection of information ▪specialised personnel training ▪other such activities

Art 35 of the Convention: 24/7 Network

A point of contact available on a twenty-four hour, seven-day-a-week basis

CONVENTION	ROMANIA
Article 35 – 24/7 Network	**Article 62 - Law on cybercrime** **The Service for Combating Cybercrime was established within the Prosecutor's Office of the High Court of Cassation and Justice** **The competences meet the requirements of the Convention on international co-operation and it is a liaison point available 24/7** **Since 26.11.2004 the service has operated within the central Directorate for Investigation of the Organized Crime and Terrorism Offences.**

Attributions:

- **Provides specialised assistance and gives information on the Romanian legislation in the domain to similar contact points in other states**
- **Orders the expeditious preservation of data as well as the seizure of the objects containing computer data or regarding traffic data required by a competent foreign authority**
- **Executes/facilitates the execution according to the law of letters rogatory in cases of combating cybercrime cooperating with all the competent Romanian authorities**

CONCLUSIONS

- Need for speeding up the mutual assistance and fostering international cooperation on cybercrime
- Harmonization of common principles that need to be applied in criminal mutual legal assistance on cybercrime
- Appropriate international instruments for cooperation - Convention on Cybercrime contains general and specific provisions meant to establish the framework for an expedited and reliable international cooperation
- Increase the use of 24/7 Network
- In order to be effective it has to be promoted and implemented globally

THANK YOU FOR YOUR ATTENTION

cristina.schulman@coe.int