Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version April 2008

# Cybercrime legislation – country profile

# ROMANIA

*This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.*

*Alexander Seger*
*Economic Crime Division*
*Directorate General of Human Rights and Legal Affairs*
*Council of Europe, Strasbourg, France*
*Tel: +33-3-9021-4506*
*Fax: +33-3-9021-5650*
*Email: alexander.seger@coe.int*
www.coe.int/cybercrime

| **Country:** | **Romania** |
|---|---|
| Signature of Convention: | Yes: 23.11.2001 |
| Ratification/accession: | Yes: 12.05.2004 |
| ***Provisions of the Convention*** | ***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)* |
| *Chapter I – Use of terms* | |
| Article 1 – "Computer system", "computer data", "service provider", "traffic data | ART. 35 of Romania Law no 161/2003<br>All the terms required by the Convention to be defined "computer system", "computer data", "service provider" and "traffic data" (article 1), "child pornography" (article 9) and "subscriber information" (article 18) are covered by Art. 35 of Law no 161/2003.<br>Romanian Law provides also for some additional definitions:<br>• *automatic data processing*<br>• *computer program*<br>• *security measures*<br>• *without right*<br><br>**General remark regarding the mental element.**<br>Under the Romanian legal system ***an act that resides in an action committed with negligence shall be an offence only when the law provides this expressly*** (article 19 paragraphs 2 Criminal Code). As a result of this provision it was stated that there is no need to specify expressly the intentional element in the text.<br>If the law **does not provide any mental element in the case of an offence consisting of an action the mental element required is** |

| | |
|---|---|
| | **intend**. |
| *Chapter II – Measures to be taken at the national level*<br>*Section 1 – Substantive criminal law* | |
| Article 2 – Illegal access | ART.42 of Romania Law no 161/2003 |
| Article 3 – Illegal interception | ART.43 of Romania Law no 161/2003 |
| Article 4 – Data interference | ART.44 of Romania Law no 161/2003 |
| Article 5 – System interference | ART.45 of Romania Law no 161/2003 |
| Article 6 – Misuse of devices | ART.46 of Romania Law no 161/2003 |
| Article 7 – Computer-related forgery | ART.48 of Romania Law no 161/2003 |
| Article 8 – Computer-related fraud | ART.49 of Romania Law no 161/2003 |
| Article 9 – Offences related to child pornography | ART.51(1) of Romania Law no 161/2003 |
| Title 4 – Offences related to infringements of copyright and related rights | |
| Article 10 – Offences related to infringements of copyright and related rights | ART. $139^{8}$ - $139^{9}$ and art. 143 of Law on copyright no.8/1996 |
| Article 11 – Attempt and aiding or abetting | For ART. 11 (1) of the Convention on Cybercrime – ART. 23, ART. 26, ART. 27 of Criminal Code<br>For ART. 11(2) of Convention on Cybercrime – ART. 47, ART.50 and ART. 51(2) of Romania Law no 161/2003 |
| Article 12 – Corporate liability | ART. $19^{1}$ of Criminal Code (amended by Law no 278/2006)<br>Article 12 – partially covered |
| Article 13 – Sanctions and measures | For art. 13(1) of Convention on Cybercrime - ART. 42-46, ART.48-49 and ART. 51 of Romania Law no 161/2003<br>For art. 13(2) of Convention on Cybercrime – ART. $53^{1}$ of Criminal Code (amended by Law no 278/2006) |
| *Section 2 – Procedural law* | |
| Article 14 – Scope of procedural provisions | ART. 58 of Romania Law no 161/2003 |
| Article 15 – Conditions and safeguards | ART. 26 (1), 27 (3), 28 of Romania Constitution, ART. $91^{1}$ Criminal procedure Code, ART. 57 (1), (2) of Romania Law no 161/2003, ART. 3 (3), (5) of Romania Law no 365/2002 on electronic commerce (amended by Law no 121/2006) |
| Article 16 – Expedited preservation of stored | ART.54 of Romania Law no 161/2003 |

| | |
|---|---|
| computer data | |
| Article 17 – Expedited preservation and partial disclosure of traffic data | ART.54 of Romania Law no 161/2003 |
| Article 18 – Production order | ART. 16 of Law no 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences |
| Article 19 – Search and seizure of stored computer data | For art. 19 (3) of Convention on Cybercrime – ART. 55 of Romanian Law 161/2003(in view of making copies that can serve as evidence); ART. 96 and Art.99 of Criminal procedure Code.<br>For art.19 (1-2) of Convention on Cybercrime - ART.56 (1) (3) of Romania Law no 161/2003. |
| Article 20 – Real-time collection of traffic data | It is considered to be implemented by the new draft of the Criminal Procedure Code |
| Article 21 – Interception of content data | ART.57 of Romania Law no 161/2003<br>ART. $91^1$ (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 |
| *Section 3 – Jurisdiction* | |
| Article 22 – Jurisdiction | ART. 3-4 and art.142-143 Criminal Code |
| *Chapter III – International co-operation* | |
| Article 24 – Extradition | Art.23-24 (1) of Convention on cybercrime - ART.60 of Romania Law no 161/2003 and Title II of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006 |
| Article 25 – General principles relating to mutual assistance | ART.61 of Romania Law no 161/2003 |
| Article 26 – Spontaneous information | ART.66 of Romania Law no 161/2003 and ART. 166 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006 |
| Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements | Single article (2) b) of Law no 64/2004 for ratification of the Council of Europe Convention on cybercrime |
| Article 28 – Confidentiality and limitation on use | ART. 12 of Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006 |
| Article 29 – Expedited preservation of stored computer data | ART.63 of Romania Law no 161/2003 |
| Article 30 – Expedited disclosure of preserved traffic data | ART.64 of Romania Law no 161/2003 |
| Article 31 – Mutual assistance regarding accessing of stored | ART. 60 of Romania Law no 161/2003 |

| | |
|---|---|
| computer data | |
| Article 32 – Trans-border access to stored computer data with consent or where publicly available | ART.65 of Romania Law no 161/2003 |
| Article 33 – Mutual assistance in the real-time collection of traffic data | ART. 60 of Romania Law no 161/2003 |
| Article 34 – Mutual assistance regarding the interception of content data | ART. 60 of Romania Law no 161/2003 |
| Article 35 – 24/7 Network | ART. 62 of Romania Law no 161/2003 |
| Article 42 – Reservations | *No need to fill in this information as it will be copied from the Council of Europe treaty data base* |

## Appendix 1: **solutions in national legislation**

### Romania Law no 161/2003

**Title III on preventing and fighting cybercrime**[1]

**Chapter I**

**General Provisions**

Art. 34 – The present title regulates the prevention and fighting of cybercrime by specific measures to prevent, discover and sanction the infringements through the computer systems, providing the observance of the human rights and the protection of personal data.

Art. 35 - (1) For the purpose of the present law, the terms and phrases below have the following meaning:

a) *„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;

b) *„automatic data processing"* is the process by means of which the data in a computer system are processed by means of a computer program;

c) *„computer program*" means a group of instructions that can be performed by a computer system in order to obtain a determined result;

d) *„computer data"* are 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;

e) *„a service provider"* is:

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

2. any other natural or legal person processing or storing computer data for the persons mentioned in paragraph 1 and for the users of the services offered by these;

f) *„traffic data"* are any computer data related to a communication by means of a computer system and generated by this, which represent a part in the chain of communication,

[1] The relevant provisions for preventing, discovering and sanctioning the offences committed through the computer systems are incorporated in Title III of the Law 161/2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, to prevent and sanction corruption (published in the Official Gazette no 279 from 21 April 2003)

indicating the communication's origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication

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;

h) *„security measures"* refers to the use of certain procedures, devices or specialised computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users;

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.

(2) For the purpose of this title, *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 competent natural or legal 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.

## Chapter II

## Prevention of cybercrime

Art. 36 – In order to ensure the security of the computer systems and the protection of the personal data, the authorities and public institutions with competence in the domain, the service providers, the non-governmental organisations and other representatives of the civil society carry out common activities and programs for the prevention of cybercrime.

Art. 37 – The authorities and public institutions with competence in the domain, in collaboration with the service providers, the non-governmental organisations and other representatives of the civil society promote policies, practices, measures, procedures and minimum standards for the security of the computer systems.

Art. 38 - The authorities and public institutions with competence in the area, in collaboration with the service providers, the non-governmental organisations and other representatives of the civil society organise informing campaigns on cybercrime and the risks the users of the computer systems.

Art. 39 – (1) The Ministry of Justice, The Ministry of Interior, the Ministry of Communications and Information Technology, Romanian Intelligence Service and Foreign Intelligence Department establish and permanent up-date a database on cybercrime.
(2) The National Institute of Criminology under the subordination of the Ministry of Justice

carries out periodic studies in order to identify the causes determining and the conditions favouring the cybercrime.

Art. 40 - The Ministry of Justice, The Ministry of Interior, the Ministry of Communications and Information Technology, Romanian Intelligence Service and Foreign Intelligence Department carry out special training programs for the personnel with attributions in preventing and fighting cybercrime.

Art. 41 – The owners or administrators of computer systems for which access is forbidden or restricted to certain categories of users are obliged to warn the users on the legal access and use conditions, as well as on the legal consequences of access without right to these computer systems.

## Chapter III

## Crimes and contraventions

### Section 1

Offences against the confidentiality and integrity of computer data and systems

Art. 42 – (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.

Art. 43 – (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.

Art. 44 – (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.

Art. 45 – 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.

Art. 46 – (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.

Art. 47 – The attempt to commit the offences provided in Articles 42-46 shall be punished.

## Section 2

## Computer-related offences

Art. 48 – 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.

Art. 49 – 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 shall be punished with imprisonment from 3 to 12 years.

Art. 50 – The attempt to commit the offences provided in Articles 48 and 49 shall be punished.

## Section 3

## Child pornography through computer systems

Art.51 – (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.

(2) The attempt shall be punished.

## Section 4

## Contraventions

Art. 52 – The non-observance of the obligation stipulated by art. 41 is a contravention and shall be sanctioned by a fee between 5.000.000 lei and 50.000.000 lei.

Art. 53 – (1) Finding a contravention provided in art. 52 and the application of the sanction are performed by the personnel authorised for this purpose by the minister of communications and IT as well as by the specially authorised personnel within the Ministry of Interior.

(2) The provisions of Government Ordinance no. 2/2001 on the legal regime of contraventions, approved with amendments by Law no.180/2002 are applicable.

## Chapter IV

## Procedural provisions

Art. 54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.

(2) During the criminal investigation, 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.

(3) The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.

(4) 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.

(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.

(6) 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.

Art. 55 – (1) Within the term provided for at art. 54 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, 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.

(2) If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body.

(3) The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the integrity of the information contained by them.

Art.56 – (1) 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.

(2) 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 and that are achieved according to art. 55, paragraph (3).

(3) 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.

(4) The provisions of the Criminal Procedure Code regarding searches at home are applied accordingly.

Art.57 – (1) 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 doers cannot be achieved on the basis of other evidence.

(2) The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed.

(3) The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 months.

(4) Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken.

(5) The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly.

Art.58 – 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.

Art.59 – For the criminal offences stipulated in this title 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.

## Chapter V

## International Cooperation

Art.60 – (1) The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is Party of, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the domain.

(2) The cooperation, organised and carried out according to paragraph (1) can have as scope, as appropriate, international legal assistance in criminal matters, extradition, the 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, as well as other such activities.

Art.61 – (1) At the request of the Romanian competent authorities or of those of other states, on the territory of Romania common investigations can be performed for the prevention and fighting the cybercrime.

(2) The common investigations referred to at paragraph (1) are carried out on the basis of bilateral or multilateral agreements concluded with the competent authorities.

(3) The representatives of the Romanian competent authorities can participate in common investigations performed on the territory of other states by observing their legislation.

Art.62 - (1) In order to ensure an immediate and permanent international cooperation in the cybercrime area, within the Organised Crime Fighting and Anti-drug Section of the Prosecutor's Office belonging to the Supreme Court, a service for combating cybercrime is established as a contact point permanently available.

(2) The Service for combating cybercrime has the following attributions:

a) provides specialised assistance and information on Romanian legislation in the area to similar contact points in other states;

b) orders the expeditious preservation of data as well as the seizure of the objects containing computer data or the data regarding the data traffic required by a competent foreign authority;

c) executes or facilitates the execution, according to the law, of letters rogatory in cases of combating cybercrime cooperating with all the competent Romanian authorities.

Art. 63 - (1) 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.

(2) The request for expeditious preservation referred to at paragraph (1) includes the following:
a) the authority requesting the preservation;

b) a brief presentation of facts that are subject to the criminal investigation and their legal background;

c) computer data required to be preserved;

d) any available information, necessary for the identification of the owner of the computer data and the location of the computer system;

e) the utility of the computer data and the necessity to preserve them;
f) the intention of the foreign authority to formulate a request of international legal assistance in criminal matters;

(3) 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;

Art.64 - If, in executing the request formulated according to art.63 paragraph (1), a service provider in another state is found to be in possession of the data regarding the traffic data, the Service for combating cybercrime will immediately inform the requesting foreign authority about this, communicating also all the necessary information for the identification of the respective service provider.

Art.65 - (1) A competent foreign authority can have access to public Romanian sources of computer data without requesting the Romanian authorities.

(2) 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.

Art. 66 – The competent Romanian authorities can send, ex-officio, to the competent foreign authorities, observing the legal provisions regarding the personal data protection, the information and data owned, necessary for the competent foreign authorities to discover the offences committed by means of a computer system or to solve the cases regarding these crimes.

Art.67 – Art.29 of Law no.365/2002 on e-commerce, published in the Official Journal of Romania, Part I, no.483 of May 7, 2002 is abrogated.

*Constitution of Romania is available in English on http://www.cdep.ro*

**CRIMINAL CODE**
**Title II**
**OFFENCES**

**Chapter I**
**GENERAL PROVISIONS**

**Guilt**

**Art.19. (1)** There is guilt when an act that represents a social danger is committed with intent or with negligence.
1. An act was committed with intent when the offender:
a) foresaw the outcome of his/her act, and intended for this outcome to take place by the commission of that act;
b) foresaw the outcome of his/her act and, although he/she did not intend it, accepts the possibility for it to take place.
2. An act was committed out of negligence when the offender:
a) foresaw the outcome of his/her act, but did not accept it, because he/she unfoundedly deemed it unlikely to take place;
b) did not foresee the outcome of his/her act, although he/she ought and would have been able to.
**(2) An act that resides in an action committed with negligence shall be an offence only when the law provides this expressly.**
(3) An act consisting of inaction shall be an offence regardless of whether it was committed with intent or with negligence, unless the law sanctions only its commission with intent.

**Chapter III**
**PARTICIPATION**

**Participants**

**Art.23 -** Persons who contribute to the commission of an act provided in the criminal law as authors, instigators or accomplices are participants.

**Authors**

**Art. 24 -** A person directly committing an act provided in the criminal law is an author.

**Instigators**

**Art.25 -** An instigator is a person who intentionally determines another person to commit an act provided in the criminal law.

**Accomplices**

**Art.26 -** (1) An accomplice is a person who intentionally facilitates or helps in any way in the commission of an act provided in the criminal law. A person who promises, either before or during the commission of the offence, to conceal the proceeds emerging from it or to favour the perpetrator, even if after commission of the offence the promise is not kept, shall also be an accomplice.

**Penalty for participation**

**Art.27** - Instigators and accomplices to an act provided in the criminal law committed with intent shall be sanctioned by the penalty provided in the law for authors. In establishing the penalty, each person's contribution to the commission of the offence, as well as Art. 72, shall be taken into account.

***THE CRIMINAL CODE amended by Law no 278/2006 (extract)***

| | |
|---|---|
| Conditions for the criminal liability of legal persons | ART. 19[1]<br>Legal persons, with the exception of the State, the public authorities and the public institutions the activity of which is not the subject of private domain, shall be criminally liable for criminal offences committed in order to activate in their activity field or in the interest or on behalf of the legal person, provided that the act has been committed with the form of guilt provided in criminal law.<br>Criminal liability of legal persons shall not exclude the criminal liability of natural persons who contributed in any manner to the perpetration of the same criminal offence." |
| Types of penalties applicable to legal persons | ART. 53[1]<br>The penalties are: main and complementary.<br>The main penalty is a fine from RON 2.500 to RON 2.000.000.<br>Complementary penalties are:<br>a) dissolution of the legal person;<br>b) suspension of the activity of the legal person for a period from 3 months to one year or suspension of that of the activities of the legal person which served in the perpetration of the offence, for a period from 3 months to 3 years;<br>c) closing of working locations belonging to the legal person, for a period from 3 months to 3 years;<br>d) prohibition to participate in public procurement for a period from one to 3 years;<br>e) display or broadcasting of the sentencing judgement. |

***CRIMINAL PROCEDURE CODE (extract)***
***Section V[1]***
***Audio or video interception and recording***

*ART. 91[1]*

Conditions and cases of interception and recording of conversations or communications by telephone or by any other electronic means of communication

The interception and recording of conversations or communications by telephone or by any electronic means of communication are performed with the reasoned authorisation of a judge, at the request of the public prosecutor who is conducting or supervising criminal prosecution, under the law, in the event that solid data or clues indicate the preparation or perpetration of a criminal offence for which criminal prosecution is conducted ex officio, and interception and recording are required in order to establish the factual situation or because it would be impossible to identify or locate the participants by any other means or such means would cause much delay to the investigation.

Interception and recording of conversations or communications by telephone or by any electronic means of communication may be authorised for criminal offences against national security, as set forth in the Criminal Code and in other special laws, as well as for criminal offences of drug trafficking, weapons trafficking and trafficking in persons, terrorist acts, money laundering, counterfeiting of currency or other valuables, for the criminal offences set forth in Law No.78/2000 on the Prevention, Detection and Punishment of Acts of Corruption, as subsequently amended and supplemented, and for other serious criminal offences or criminal offences that are perpetrated through means of electronic communication. Para. 1 shall apply accordingly.

Authorisation shall be given for the period of time during which interception and recording is needed, however not for more than 30 days, in private by the president of the court that would be competent to try the case in first instance or of the court of the same rank that has jurisdiction over the prosecution office where the public prosecutor works who is conducting or supervising criminal prosecution. In the absence of the president of the court, the authorisation shall be given by a judge designated by the court president.

Such authorisation may be renewed, either before or after the previous one expires, but under the same conditions and for properly justified reasons. However, each extension may not exceed 30 days.

The total duration of authorised interception and recording, with regard to the same person and the same act may not exceed 120 days.

Recording of conversations between a lawyer and the party whom he is representing or assisting within the proceedings may not be used as evidence unless it contains or leads to the establishment of conclusive and useful data or information regarding the preparation or commission by the lawyer of a criminal offence of those provided in para. 1 and 2.

The public prosecutor ordains immediate cessation of interceptions and recordings before the expiry of the authorisation if the reasons that justified such measures no longer exist, and shall inform about this the law court that issued the authorisation.

At the reasoned request of the injured person, the public prosecutor may request authorisation from the judge to intercept and record conversations or communications by the injured person by telephone or by any electronic means of communication, whatever the nature of the criminal offence under investigation.

Interception and recording of conversations or communications shall be authorised by means of a reasoned order, which must include: the actual clues and facts that justify the measure; the reasons for which it would be impossible to determine the factual situation or to identify or locate the participants by other means or the reasons why the investigation would be very much delayed; the person, the means of communication or the place that is subject to recording; and the period for which interception and recording are authorised.

**Law no. 508/2004 on establishing, organizing and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences *(amended by Emergency Ordinance of Government no. 131/2006).***

***ART. 16***

(2) The public prosecutors of the Directorate for Investigation of Offences of Organised Crime and Terrorism may ordain that they be communicated the originals or copies of 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, under paragraph (1).

(3) Failure to observe the obligation in paragraph (2) shall entail judicial liability, under the law.

***CRIMINAL PROCEDURE CODE (extract)***

| | |
|---|---|
| **Confiscation of objects and writings** | **Art. 96 -** The criminal investigation body or the court must take away the objects or writings that may serve as means of evidence in the criminal trial. |
| **Confiscation by force of objects or writings** | **Art. 99 –** If the object or writing required is not delivered voluntarily, the criminal investigation body or the court order confiscation by force.<br>During the trial, the order of confiscation by force of objects or writings is communicated to the prosecutor, who takes enforcement measures through the criminal investigation body. |

**THE CRIMINAL CODE (extract)**

**Criminal Law personality**

**Art.4.** Criminal law shall apply to offences perpetrated outside the Romanian territory, if the perpetrator is a Romanian citizen or if he/she, while having no citizenship, domiciles in this country.

Decisions of the Constitutional Court:

**Territorial nature of Criminal Law**

**Art.3.** Criminal Law shall apply to offences committed on Romanian territory.

**Territory**

**Art. 142.** The term "territory" in the phrases "Romanian territory" and "the territory of our country" means the surface of land and water that is comprised by the borders, with the subsoil and the aerial space, as well as the territorial sea with its soil, subsoil and aerial space.

**Offence committed on the territory of our country**

**Art. 143.** (1) "Offence committed on the territory of our country" means any offence committed on the territory shown in Art. 142 or on Romanian ships or aircraft.

(2) An offence shall be deemed as committed on the territory of our country also when only an act of realisation was performed or only the result of the offence occurred on this territory or on Romanian ships or aircraft.

**Law no 64/2004 for ratification of the Council of Europe Convention on cybercrime**

In accordance with Article 27, paragraph 2.c, of the Convention, Romania declares that the central authorities responsible for sending and answering requests for mutual assistance are:

a) the Prosecutor's Office to the High Court of Cassation and Justice for the requests of judicial assistance formulated in pre-trial investigation (address: Blvd. Libertatii nr. 12-14, sector 5, Bucharest);

b) the Ministry of Justice for the requests of judicial assistance formulated during the trial or execution of punishment.

***The Romanian Copyright Law No.8/1996 (extract)***

ART. 139^8

There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the act of making available to the public, including through the Internet or other computer networks, without the consent of the owners of the copyright of protected works, neighbouring 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 it from anywhere or at anytime individually chosen.

ART. 139^9

There is a criminal offence and shall be punished with imprisonment from 1 to 4 years or a fine the unauthorised reproduction in information systems of computer software in any of the following ways: install, storage, running or execution, display or intranet transmission.

ART. 143

(1) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of manufacturing, import, distribution or rental, offer, by any means, for sale or rental or possession in view of selling without right devices or components that allow neutralisation of technical measures of protection or that perform services that lead to neutralisation of technical measures of protection or that neutralise such technical measures of protection, including in the digital environment.

(2) There is a criminal offence and shall be punished with imprisonment from 3 months to 3 years or a fine the act of person whom, without having the consent of the owners of the copyright, and while knowing or should have known that thus is allowing, facilitating, causing or concealing a violation of a right as set forth in this law:

a) removes or modifies from the protected works for commercial purposes any electronic information relating to the applicable regulations on copyright or neighbouring rights,

b) distributes, imports in view of distribution, broadcasts or publicly communicates or makes available to the public, so as to allow access from any place and at any time chosen individually, without right, through digital technology, works or other protected works for which the information existing in electronic form regarding the regulations on copyright or related rights, have been removed or modified without authorisation.