

Anti-corruption law

Title III

on preventing and fighting cyber-crime

Chapter I

General Provisions

Art.34 – The present title regulates the prevention and fighting of cyber-crime, 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 programme;
 - b) „ automatic data processing” is the process by means of which the data in a computer system are processed by means of a computer programme;
 - c) „computer programme” 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 programme 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 at item 1 and for the users of the services offered by these;
 - f) „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;
 - 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 programmes 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 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.
- (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 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.

Chapter II

Prevention of cyber-crime

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 programmes for the prevention of cyber-crime.

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 domain, in collaboration with the

service providers, the non-governmental organisations and other representatives of the civil society organise informing campaigns on cyber-crime and the risks the users of the computer systems.

Art.39 – (1) The Ministry of Justice, The Ministry of Domestic Affairs and the Ministry of Communications and Information Technology draft and up-date a database on cyber-crime.

(2) The National Institute of Criminology under the subordination of the Ministry of Justice carry out periodic studies in order to identify the causes determining and the conditions favouring the cyber-crime.

Art.40 - The Ministry of Justice, The Ministry of Domestic Affairs and the Ministry of Communications and Information Technology carry out special training programmes for the personnel with attributions in preventing and fighting cyber-crime.

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 data and computer systems

Art.42 – (1) The illegal access to a computer system is a crime and is punished with imprisonment from 6 months to 3 years.

(2)

(3) If the fact mentioned at item (1) is performed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.

Art.43 – (1) The illegal interception of any transmission of computer data that is not published 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 is applied also for the illegal interception, of electromagnetic emissions from a computer system carrying non-public computer data.

Art.44 – (1) The illegal alteration, deletion or deterioration of computer data of the access restriction to such data is considered 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 unauthorised data transfer by means of an information data storing mean is also punished as in paragraph (2).

Art.45 – The serious hindering, without right, of a computer system operation, by the introducing, transmitting, altering, deleting or deteriorating computer data or by restricting the access to these data is considered a criminal offence and is punished with imprisonment from 3 to 15 years.

Art.46 – (1) The following are considered criminal offences and punished with imprisonment from one to 6 years.

a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer programme designed or adapted for the purpose of committing one of the offences established in accordance with arts.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 one of the offences established in accordance with arts.42-45;

(2) The possession, without right, of a device, computer programme, password, access code or computer data referred to at paragraph (1) for the purpose of one of the offences established in accordance with arts.42-45 is also punished similarly.

Art.47 – The intent to commit the offences referred to in arts.42-43 is also 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 these data, resulting in inauthentic data, with the intent to be used for legal purposes, is considered a criminal offence and is punished with imprisonment from 2 to 7 years.

Art.49 – Causing the loss of property to a person by the input, alteration or deletion of computer data, by restricting the access to such data or by preventing in any way the operation of a computer system, in order to obtain an economic benefit for oneself or for another is punished with imprisonment from 3 to 12 years.

Art.50 – The intent to commit the offences referred to in arts.48 and 49 is also punished.

Section 3

Child pornography through computer systems

Art.51 – (1) Producing for the purpose of its distribution, offering or making available, distributing or transmitting, procuring for oneself or another of child pornography material, or possessing, without right, child pornography material within a computer system or computer data storing device is considered a criminal offence and is punished with imprisonment from 3 to 12 years.

(2) The intention is punished.

Section 4

Contraventions

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

Art.53 – (1) Finding a contravention mentioned in art.52 and the application of sanctions, 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 Domestic Affairs.

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

Chapter IV

Procedural provisions

Art.54 - (1) In urgent and duly 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 disposed.

(2) During the criminal investigation, the preservation is disposed by the prosecutor by a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court settlement.

(3) The measure referred to at paragraph (1) is disposed 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 settlement is sent, at once, 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) 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.

(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 disposes on the seizing of the objects containing computer data, data regarding data traffic 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 disposes the forced seizure. During the trial, the forced seizure disposition 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 dispose a search.

(2) If the criminal investigation body or the court appreciates 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 dispose performing copies that would serve as evidence and that are achieved in agreement with 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, the authorisation can be disposed at once to perform 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 advise, 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 procedures of this chapter are applied in criminal investigations or the judgment of cases regarding the criminal offences stipulated by the present law or any other criminal offences carried out by means of computer systems.

Art.59 – For the criminal offences referred to by this law and any criminal offences carried out by means of computer systems, in order to ensure the special seizure stipulated at art.118 of the Criminal Code prevention measures can be taken that are 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 part 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 se common investigations can be performed for the prevention and fighting the cyber-crime.

(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 cyber-crime domain, within the Organised Crime Fighting and Anti-drug Section of the prosecutor's Office belonging to the Supreme Court, a cyber-crime fighting service is created as a contact point available permanently.

(2) The Cyber-Crime Fighting Service has the following attributions:

- a) provides specialised assistance and offers data on the Romanian legislation in the domain and similar contact points in other states;
- b) disposes 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 mandated commissions solicited in cases of cyber-crime fighting, cooperating with all the competent Romanian authorities.

Art.63 - (1) Within the international cooperation, the competent foreign authorities can require from the Cyber-Crime Fighting Service the expeditious preservation of the computer data or of the data regarding the data traffic 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 data traffic, Cyber-Crime Fighting Service will immediately advise 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 the necessity of formulating a request in this sense to 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 information system, without the necessity of formulating a request in this sense to 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 crimes made by means of information systems or to solve the causes 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.