Co-funded by the
Erasmus+ Programme
of the European Union

STRATEGIC PARTNERSHIP BETWEEN SCHOOLS
KA2 ACTION, ERASMUS+ PROGRAM
THE VIRTUAL UNIVERSE WE WANT
PROJECT NO: 2016-1-RO01-KA219-024515

ROMANIA

IT LEGISLATION IN ROMANIA

Romania has many laws that govern the use of the Internet

- E-commerce
- Copyright
- Electronic documents
- Electronic payments
- Online advertisting
- Protection of personal data
- Computer crime
- Online pornography
- Electronic communications
- Electronic government
- Internet video services

Romanian Constitutional Court decision no. 1258 from 8 October 2008 regarding the unconstitutionality exception of the provisions of Law no.298/2008

Art.1 – *„(1) The present law established the obligation of the electronic communication providers of services and public networks to retain certain data produced or processed during their activity of providing electronic communication services, in order to make them available to the competent authorities to use them in activities of enquiry, detection and proceedings against serious crimes.*

(2) The present law is applied to traffic and localisation data of the physical and legal persons, as well as to the related data necessary to identify the subscriber or the registered user.

(3) The present law does not apply to the content of the communication or information accessed while using an electronic communication network.

(4) The enforcement of the present law shall be done by respecting law 677/2001 for people's protection on processing personal data and the free movement of these data, with the subsequent modifications, as well as law 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area, with the subsequent changes."

Art.15 – „The public network communication providers and the electronic communication services providers have the obligation, at the request of the competent authorities, based on the authorization issued according to art 16, to send forthwith the retained data to these authorities according to the present law, with the exception of the force majeure cases."

Law on on the processing of personal data and the protection of privacy in the electronic communications sector

Number 506/2004

Article 2

Definitions

(1) For the purposes of this Law, the following definitions shall apply:

a) user – any natural person using a publicly available electronic communications service, without necessarily having subscribed to this service;

b) traffic data – any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

c) location data – any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

d) communication – any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service; this does not include the information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

e) call – a connection established by means of a publicly available telephone service allowing two-way communication in real time;

f) value added service – any service which requires the processing of traffic data or location beyond what is necessary for the transmission of a communication or the billing thereof;

g) electronic mail – service consisting in conveyance on a public electronic communications network of any text, voice, sound or image message, which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

(2) For the purposes of this Law, the definitions set out in Art. 3 letters a), b), c) and i) of Law no. 677/2001, in Art. 2 letters a), b), c) and h) of Government Ordinance no. 34/2002 on the access to the public electronic communications networks and to the associated infrastructure, as well as their interconnection, approved with amendments and completions by Law no. 527/2002, in Art. 2 paragraph (1) letter b) of Government Emergency Ordinance no. 79/2002 on the general regulatory framework for communications, approved with amendments and completions by Law no. 591/2002, Art. 1 points 1 and 8 of Law no. 365/2002 on the electronic commerce, with the subsequent amendments, and in Art. 2 paragraph (1) letter c) of the Law no. 304/2003 on the universal service and users' rights relating to the electronic communications networks and services shall also apply.

Article 3

Security measures

(1) The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its service. With respect to network security, if necessary, the provider of the publicly available electronic communications service shall take those security measures in conjunction with the provider of the public electronic communications network. Having regard to the state of the art and the cost of their implementation, the measures taken shall ensure a level of security appropriate to the risk presented.

(2) The National Regulatory Authority for Communications, hereinafter referred to as ANRC, shall establish the conditions under which the providers must fulfil the obligation set out in paragraph (1).

(3) In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must:

a) inform the subscribers of such risk and of the possible consequences ensuing;

b) inform the subscribers of any possible remedies;

c) inform the subscribers of the likely costs involved by eliminating the risk.

Article 5

Traffic data

(1) Traffic data relating to subscribers and users, processed and stored by the provider of a public electronic communications network or by the provider of a publicly available electronic communications service, must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs (2), (3) and (5).

(2) Traffic data necessary for the purposes of subscriber billing and interconnection payments may only be processed up to the end of a period of 3 years from the due date of the corresponding payment obligation.

(3) For the purpose of marketing its electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph (1) only to the extent and for the duration necessary for such services or marketing, and only if the subscriber or user to whom the data relate has previously given his/her express consent. The subscriber or user shall be given the possibility to withdraw his/her consent for the processing of traffic data at any time.

(4) In the cases referred to in paragraphs (2) and (3), the provider of the publicly available electronic communications service must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing. In the case referred to in paragraph (3), this information must take place prior to obtaining the consent of the subscriber or user.

(5) Processing of traffic data, in accordance with paragraphs (1) to (4), may only be carried out by the persons acting under the authority of the providers of public electronic communications networks or publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing value added services, and is allowed only to the extent it is necessary for the fulfilment of these duties.

(6) Paragraphs (1) to (3) and (5) shall apply without prejudice to the possibility for competent bodies to have access to traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Anti-corruption law 161/2003

Published in the Official Monitor on 21/04/2003

Title III
on preventing and fighting cyber-crime

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) 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 date 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 punish 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 fro 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.942-45 is also punished similarly.

Art.47 – The intent to commit the offences referred to in arts.42-43 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.

Law on the prevention and fighting of pornography
No 196/2003

- aspects regarding Internet-

Art. 8. - (1) The natural and legal persons creating pornographic sites
are obliged to password them, and the access to these will be allowed only after paying a fee per using minute, established by the creator of the site and declared at the fiscal bodies.
(2) The natural and legal persons creating or administering sites have to clearly emphasize the number of accesses to the respective sites in order to be subjected to the fiscal obligations provided by the law
(3) The activities mentioned in this article are authorised by a commission of the Ministry of Culture and Cults, with representatives from the Ministry of Domestic Affairs and Information Technology and Communications Ministry..
(4) The creation and administration of pedophilic, zoophilic or necrophilic sites are forbidden.

Art. 15. - (1) The National Regulatory Authority on Communications (ANRC) can receive claims regarding the non-compliance to the provisions of art. 8.
(2) In case of receiving such claims and after checking the contents of the site, ANRC requires the Internet service providers to block the access to the respective site.
(3) The non-compliance of the Internet service providers to the obligation of blocking the access to the sites that do not observe the provisions of art. 8, within 48 hours from the receipt of the request mentioned at paragraph (2) from ANRC, is an infringement and is penalised with a fine from 100.000.000 lei
to 500.000.000 lei.

Art. 19. - Within 30 days from publishing this law in the Official Journal of Romania
the Ministry of Culture and Cults, the Ministry of Education and Research, the Ministry of Domestic Affairs and MCTI will elaborate the application norms for this law, that will be approved by a Government decision, giving in detail the procedure to obtain the necessary approvals for the operation of the restaurants, for the creation of Internet sites, as well as the structure and operation of the commissions provided by this law.

Law on the Electronic Signature
- no. 455/2001 -

SECTION TWO
Definitions

Art. 4. For the purpose of this law:
Data in electronic form means information supplied in a conventional form appropriate for creating, processing, sending, receiving or storing that information by electronic means.
Document in electronic form means a collection of logically and operationally interrelated data in electronic form that reproduces letters, digits or any other meaningful characters in order to be read through software or any other similar technique.
Electronic signature means data in electronic form, which are included in, attached to or logically associated with a document in electronic form and serve as a method of identification.
Extended electronic signature means an electronic signature which meets all the conditions specified below:
a. it is uniquely linked to the signatory;
b. it allows the identification of the signatory;
c. it is created using means that the signatory can maintain under his sole control;
d. it is linked to the data in electronic form to which it relates in such a manner that any subsequent change of that document is detectable.
Signatory is a person who holds a signature-creation device and acts either on his own behalf or on behalf of a third party he or she represents.
Signature-creation data means unique data in electronic form, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Law no.365 of 7 June 2002 on electronic commerce

Art.1:Definitions

For the purpose of this law, the following terms are defined as follows:
information society service – any activity of providing services or that involve the creation, modification, transfer or termination of a real right on a fixed or non-fixed asset, activity carried out by electronic means, that shows the following characteristics:a) it is performed considering a patrimony interest provided to the supplier usually by the recipient;
b) the supplier and the recipient do not have to be physically present simultaneously at the same place;
c) it is carried out by transmitting the information at the individual request of the recipient;

Art.2: Scope and application field

(1) The present law has as purpose to establish the conditions of supplying information society services as well as to establish as infringements certain deeds regarding the safety of the domains used for electronic commerce, the issuing and use of electronic payment instruments as well as the use of identification data to carry out financial operations, in order to provide a favourable framework for the free movement of these services and the development of safety conditions for them.
(2) For the purpose of this law, the activities that do not meet the elements of definition provided for at art.1, item 1 are not considered information society services, especially the following:
a) the service offer requiring the physical presence of the provider and of the recipient, even if the respective services involve the use of electronic equipment;
b) the service offer implying handling of fixed assets by the recipient even if the respective services imply the use of electronic equipment;
c) goods or services offer that is presented to the recipient by sending the information at individual request and is not meant for simultaneous reception by an unlimited number of people (point-multipoint);
d) activities performed by means of vocal telephonic services, tele-fax, telex, radio and television services, including tele-text services;
e) vocal telephony, tele-fax or telex services;
f) information exchange by means of electronic mail or other equivalent individual means between people acting in other purposes than their commercial or professional activities;
g) contractual relationship between an employee and his (her) employer.

Romanian Law on Copyright and Neighboring Rights

CHAPTER I
Introductory Provisions

Art. 1.(1) The copyright in a literary, artistic or scientific work and in any similar work of intellectual creation shall be recognized and guaranteed as provided in this Law. That right vests in the author and embodies attributes of moral and economic character.
(2) A work of intellectual creation shall be acknowledged and protected, independently of its disclosure to the public, simply by virtue of its creation, even though in an unfinished form.

Art. 2. Recognition of the rights provided for in this Law shall not prejudice or exclude protection granted under other statutory provisions.

CHAPTER II
Ownership of Copyright

Art. 3.(1) The natural person or persons who created the work shall be the author thereof.
(2) In cases expressly provided for by law, legal entities and natural persons other than the author may benefit from the protection granted to the author.
(3) Ownership of copyright may be transferred as provided by law.

Convention on Cybercrime Budapest, 23.XI.2001

Ministers or their representatives from the 26 following Member States signed the treaty: Albania, Armenia, Austria, Belgium, Bulgaria, Croatia,Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, "the Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom. Canada, Japan, South Africa and the United States, who took part in the drafting, also signed the treaty on 23 11 2001 . Other non-member States may also be invited by the Committee of Ministers to sign this treaty at a later date.

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation.