

*Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law*

ROMANIAN NATIONAL REPORT*

Tudorel TOADER - Ioana VASIU - Constantin DUVAC*

(A) Scope of questionnaire

The Romanian specialists in criminal law have the same beliefs that society of today transforms too quickly and that the information and knowledge have become key resources of the information society, affecting both the social and political structure of the society and of the state as well as the function, structure and content of the system of justice penal. We can say that we are witnessing a true revolution with a formidable social impact on the social organisation of which the criminal justice system is a part.

Regarding Romania, all these transformations of the society are at the beginning, including the replacement of the traditional structure of authority by an alternative method of control upon the society (namely the transition from nation-state to the network state).

In this light, we will respond to problems covered in this national report.

(B) Legislative Practices and Legal Concepts

(1) Computer crimes not foreseen in the Romanian Criminal Code in force (issued on 1 January 1969), but are sanctioned by a special criminal law which is Law no. 161/2003 on measures to ensure transparency in exercising public dignities, public functions and business environment, preventing and sanctioning corruption. This law provides in art. 42-47 offenses against confidentiality and integrity of data and systems, in art. 48-50 Cybercrime and in art. 51 child pornography by computer systems.

(2) The frequency of such crimes committed on Romanian territory and their consequences have determined the Romanian legislator, in 2009, to codify them, with the occasion of the adoption of Law no. 286/2009 on the Criminal Code, which, according to Law no. 187/2012 for the implementation of Law no. 286/2009 on the Criminal Code will come into force on 1 February 2014. Court decisions have influenced (but not significantly) the wording of incriminating texts of this type of antisocial acts in the new Penal Code, special limits of punishment remaining pretty high.

(3) From the date of its development to the present, Law No. 161/2003 has been amended 16 times, without being issued a new regulation. In 2009, the Romanian legislator has decided to incriminate these offenses within the new Criminal Code, the texts being taken from Law no. 161/2003 being improved in relation to the developments in jurisprudence.

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* University Professor Ph.D. Tudorel TOADER, University Professor Ph.D. Ioana VASIU, Associate Professor Ph.D. Constantin DUVAC

(C) The Specific Cybercrime Offenses

(1) All offenses relating to "cybercrime" can only be committed intentionally, directly or indirectly, and most such as that provided in Art. 48 of Law no. 161/2003¹ or illegal access to a computer system in order to obtain computer data (art. 42 par. 2 of the Law no. 161/2003) cannot be achieved without the direct intention, classified by purpose.

(2) These intentional offenses are not punishable when committed by negligence. According to art. 19 par. 2 of the Romanian Penal Code in force, "the deed consisting of a negligent act committed is an offense only when the law expressly provides that"

(3) It is not the case.

(a) Integrity and functionality of the IT system

1. According to art. 42 of Law no. 161/2003: "(1) access without right to a computer system is an offense punishable by imprisonment from 3 months to 3 years or a fine. (2) An act provided for in par. (1), committed for the purpose of obtaining computer data is punishable by imprisonment from 6 months to 5 years. (3) If the offense referred to in par. (1) or (2) is committed in violation of security measures, the punishment is imprisonment from 3 to 12 years. "

2. Article 35 of Law no. 161/2003:

a. "a) computer system means any device or assembly of devices interconnected or in a functional relation, of which one or more provides automated data processing, using a computer program; c) computer program means a set of instructions that can be executed by a computer system to achieve a specific result; d) computer data means any representation of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can determine the execution of a function by a computer system. "

b. i. Article 44 of Law no. 161/2003: "(1) An act to modify delete or damage data or restrict access to the data, is considered a crime and is punishable by imprisonment from 2 to 7 years. (2) The unauthorized data transfer from a computer system shall be punished with imprisonment from 3 to 12 years. (3) With The penalty provided in para. (2) is sanctioned the unauthorized transfer of data from a data storage device." Article 45 of Law no. 161/2003: "Anyone serious hindering without right, the operation of a computer system by inputting, transmitting, modifying, deleting or damage to data or by restricting access to data is an offense punishable by imprisonment from 3 to 15 years."

b. ii. Article 43 of Law no. 161/2003: "(1) interception without right, of a data that is not public information and is intended for a computer system, such a system comes from or is made in a computer system is a crime punishable by imprisonment for 2-7 years. (2) With the same punishment is sanctioned the interception without right, of electromagnetic emissions from a computer system that contains non-public information".

¹ Article 48 - The input, modify or delete, without right to restrict computer data without right, access to these data, resulting in inauthentic data, in order to be used in order to produce legal consequences, is offense punishable with imprisonment from 2 to 7 years.

3. Data Forgery

Article 48 of Law no. 161/2003: "The input, modify or deletion, without right, of computer data or to restrict without right, access to these data, resulting in inauthentic data, in order to be used to produce legal consequences, is an offense and is punished with imprisonment from 2 to 7 years. "

4. Misuse of Devices

Article 46 of Law no. 161/2003: "(1) Is an offense punishable 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 software designed or adapted for the purpose of committing any of the offenses referred to in art. 42-45; b) The production, sale, import, distribution or making available in any other form without the right, of a password, access code or other such computer data allowing total or partial access to an information system to commit one of the offenses referred to in art. 42-45. (2) With the same punishment is sanctioned the possession, without right, of a device, software, password, access code or computer data under par. (1) with the purpose of committing any of the offenses referred to in art. 42-45 ".

(b) Privacy

1. Violation of Secrecy of Private Data

The Law 287/2009 of the New Civil Code republished in Official Gazette 505/201 with effect from 1 October 2011 mentions the following provisions regarding the private life:

Article 71, Right to privacy: (1) Everyone has the right to respect for his private life. (2) No one shall be subjected to any interference in private life, personal or family, or the domicile, residence or correspondence, without his consent or without respecting the limits laid down in Art. 75. (3) It is also prohibited from using, in any manner, correspondence, manuscripts or other personal documents and information from the privacy of a person without their consent or without respecting the limits laid down in Art. 75.

Article 72, Right to dignity: (1) Everyone has the right to respect for his dignity. (2) Any breach of the honour and reputation of a person without consent or without respecting the limits laid down in Art. 75.

Article 73, Right to their own image: (1) Everyone has the right to their own image. (2) In exercising the right to self-image, it can prohibit or hinder reproduction, in any manner, physical appearance or his voice or, where appropriate, the use of such reproductions. Provisions of art. 75 remain applicable.

Article 74, Violations of privacy: Subject to the provisions of art. 75, can be considered as violations of privacy:

- a) entering or remaining in the dwelling or taking without right of this object without the consent of any person who lawfully occupies it;
- b) the interception without right of a private conversation, committed by any technical means, or used, knowingly, to such interception;
- c) capture or use of the image or voice of a person in a private space, without their consent;

- d) dissemination of images of the inside of a private space without the consent of the person who lawfully occupies;
- e) keeping private life under observation by any means, except for the cases provided by law;
- f) dissemination of news, debates, surveys and reports written or audio-visual on intimate, personal or family, without the consent of the person concerned;
- g) provision of materials containing images of a person to treatment in medical facilities as well as personal data concerning health, diagnosis, prognosis, treatment, circumstances related to disease and other related offenses, including autopsy results, without the consent of the person concerned, and if it is dead without the family or persons entitled;
- h) use in bad faith, the name, image, voice or likeness of another person;
- i) the dissemination or use of correspondence, manuscripts or other personal documents, including the domicile, residence, and telephone numbers of a person or family members without the consent of the person to whom they belong or, where applicable, has right to dispose of them.

2. Violation of professional confidentiality

Art. 196 of the Romanian Criminal Code provides that: (1) Disclosure, without right, of data by a person to whom they were entrusted, or which he/she learned by virtue of profession or office, if the act is likely to cause prejudice to a person, shall be punished by imprisonment from 3 months to 2 years or by fine. (2) Criminal action is initiated upon prior complaint from the injured person. (3) Reconciliation of parties removes criminal liability.

Prosecuting the deed described in art. 196 of the Romanian Penal Code aims to protect that dimension of the right to have some secrets which are to be kept exclusive by professionals and officials who have known under the public benefits to which they are bound by the exercised profession or function.

Special legal object is to those social relations on freedom of the person, from the point of view of its right to have the custody of secrecy by virtue to which turned profession or duties.

Active subject is described by text, i.e. a person who exercises or performs any function or profession entrusted under or may ask to be given the secret of the person who use its services.

Material element is represented by an action or inaction of disclosure (e.g. leaving in sight, deliberately, by the secret bearer of a secret document).

b. Subject – Type of perpetrators

Article 79 of the Romanian Criminal Procedure Code provides that: Listening of the person bound to professional secrecy: The person bound to professional secrecy cannot be heard as a witness on the facts and circumstances of which he became aware in the exercise of their profession without the consent of the person or unit to which it is bound to secrecy. A witness takes precedence over the quality of counsel, on the facts and circumstances that he knew before becoming counsel or representative of either.

The categories of persons bound to professional secrecy are expressly mentioned in the legal norms that regulates their activity, such as Law no. 213/2004 on the profession of psychologist as free practice, establishment, organization and functioning of the College of Psychologists of Romania

3. Illegal processing of personal and private data

The legal norm regulating these are is the law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed, which has the following relevant provisions:

Article 2: Scope (1) The present law applies to personal data processing, performed, totally or partially, through automatic means, as well as to the processing through means other than automatic ones, which are part of, or destined to, a personal data filing system.

(4) The law applies to the processing of personal data, carried out by Romanian or foreign natural or legal persons of public or private law, regardless of the fact that the data processing takes place in the public or private sector.

For the purposes of this law, the following terms are defined as follows:

a) personal data: - any information referring to an identified or identifiable person; an identifiable person is a person that can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific factors of his physical, physiological, psychological, economic, cultural or social identity;

b) personal data processing: - any operation or set of operations that is performed upon personal data, by automatic or non-automatic means, such as collecting, recording, organizing, storing, adapting or modifying, retrieval, consultation, use, disclosure to third parties by transmission, dissemination or by any other means, combination, alignment, blocking, deletion or destruction;

Article 5: Conditions of Legitimacy Regarding the Data Processing

(1) Any personal data processing, except for the processing which refer to the categories mentioned in Article 7 paragraph (1) and Articles 8 and 10, may be carried out only if the data subject has given his/her express and unequivocal consent for that processing.

(2) The data subject's consent is not required in the following situations:

a) when the processing is required in order to carry out a contract or an agreement previous to that contract to which the data subject is party of, or in order to take some measures, at his request, before signing that contract or previous agreement;

b) when the processing is required in order to protect the data subject's life, physical integrity or health or that of a threatened third party;

c) when the processing is required in order to fulfill a legal obligation of the data controller;

- d) when the processing is required in order to accomplish some measures of public interest or regarding the exercise of public official authority prerogatives of the data controller or of the third party to which the data are disclosed;
 - e) when the processing is necessary in order to accomplish a legitimate interest of the data controller or of the third party to which the data are disclosed, on the condition that this interest does not prejudice the interests, or the fundamental rights and freedoms of the data subject;
 - f) when the processing concerns data which is obtained from publicly accessible documents, according to the law;
 - g) when the processing is performed exclusively for statistical purposes, historical or scientific research and the data remain anonymous throughout the entire processing;
- (3) The provisions of paragraph (2) do not infringe the legal texts that govern the obligations of public authorities to respect and protect intimate, family and private life.

Article 7: Processing Special Categories of Data (1) Processing personal data regarding ethnic or racial origin, political, religious or philosophical beliefs or those of similar nature, trade-union allegiance, as well as personal data regarding the state of health or sex life, is prohibited.

Article 8: Processing of Personal Data with an Identification Function

(1) The processing of the personal identification number or of other personal data with a general identification function may be carried out only if:

- a) the data subject has given his/her express and unequivocal consent; or
- b) the processing is expressly stated by a legal provision.

(2) The supervisory authority may establish other situations in which the processing of data stated in paragraph (1) may be carried out, only after adequate guarantees have been provided in order to observe the data subject's rights.

Article 31: Failure to Notify and Malevolent Notification

Failure to submit the compulsory notification under the terms set out by Article 22 or Article 29 paragraph (3), as well as incomplete notification or one that contains false information, if the respective maladministration falls short of a criminal offense, are considered minor offenses liable to a fine of 5 million to 100 million ROL (Romanian currency – lei).

Article 32: Illegal Processing of Personal Data

The processing of personal data by a controller or by an empowered person of the data controller, breaching the provisions of Articles 4-19, or while disregarding the rights set out in Articles 12- 15 or in Article 17 is considered a minor offense if the respective maladministration falls short of a criminal offense and is fined from 10 million to 250 million ROL.

Article 33: Failure to Fulfill the Obligations Regarding the Confidentiality and Enforcement of Security Measures

Failure to fulfill the obligations regarding the enforcement of the security measures provided by Articles 19 and 20 and the confidentiality is a minor offense, if the respective maladministration falls short of a criminal offense and is liable to a fine of 15 million to 500 million ROL.

Article 34: Refusal to Supply Information

The refusal to supply the requested information or documents to the supervisory authority in the exercise of his investigative powers set out by Article 27 is considered a minor offense, if the respective maladministration falls short of a criminal offense and is liable to a fine of 10 million to 150 million ROL.

Article 35: Ascertaining Infringements and Applying Sanctions

(1) Ascertaining an infringement and applying sanctions are carried out by the supervisory authority, which may delegate these powers on to a member of staff and also by the empowered representatives of the bodies with supervising or control powers in their legal competence.

(2) The provisions of the present law regarding the infringements are complementary to those of the Government Ordinance No. 2/2001 on the legal framework of minor offenses, when the present law does not state otherwise.

(3) The minutes that report infringements and establish the sanctions may be appealed against in the administrative section of a court of law.

4. Identity theft

Forged identity is incriminated in Art. 293 of the Romanian Penal Code, as follows: (1) The act of presenting oneself under a false identity or the act of ascribing such an identity to another person, in order to mislead or maintain the deceit of a body or institution of the State or of another unit in Art. 145, in order to produce legal consequences for oneself or for another, shall be punished by imprisonment from 3 months to 3 years. (2) The same penalty shall sanction also the act of handing over a document that proves civil status or identification, in order for it to be used without right.

Forgery of identity is the deed of a person who presents himself under a false identity or attributes to another person such an identity to induce or maintain in error a public authority in order to produce legal consequences.

Forgery of identity as it is treated is also the deed of entrustment of a document that can serve as proof of identity to be used unfairly.

Offenses regarding virtual identities of users: Although there is no special legislation in this area other existing offenses are in force such as: alteration of computer data, computer fraud, etc.

Regarding the criminalization of the possession and creation of specific virtual images and the violation of the copyright law in the virtual sphere, according to the Romanian legislation, we can mention:

Within the Romanian legislation there is a special offense on child pornography. According to art. 51 of Law 161/2003 the perpetrator is 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.

(b) Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

These deeds are not explicitly foreseen as offense within the Romanian legislation. These conducts will be considered offenses with the occasion of the adoption of Law no. 286/2009 on the Criminal Code, which, according to Law no. 187/2012 for the implementation of Law no. 286/2009 on the Criminal Code will come into force on 1 February 2014.

(c) Protection Against Illegal Content ICT Related

According to article 51 of the Romanian Law no. 161 of 2003 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 is a criminal offence punished with imprisonment from 3 to 12 years and denial of certain rights. The attempt shall be punished.

In the same matter article 11 of the Law no. 196 of 2003 on preventing and combating pornography establishes that: "(1) distribution of obscene materials, presenting images of sexually explicit conduct with a minor is punishable by 1 to 5 years. (2) The same punishment shall be punished and possession of materials provided in par. (1), for their spread. "

2. Act – creation/accession/possession/transfer/public distribution by ICT

(d) ICT Related Violations of Property, Including Intellectual Property

The Law no. 8/1996 establishes offenses relating to the protection of copyright law. For example, art. 139-8 provides as an offence punishable by 1 to 4 years of imprisonment or a fine, setting available, including through the Internet or other computer networks and in the absence of the consent of the holders, works or products covered by the copyright law by the rights or the rights of producers of databases, so that the public can have access to these works or products in the place and at the time of his choosing.

(e) The Romanian criminal law does not criminalize such manifestations, explicitly.

(f) Non-compliance Offenses

Yes there is such an obligation within the Romanian legislation. The law no. 82/2012 regarding the retention of general data or data processed by the electronic communications public networks providers and electronic communications for public use providers was published in the Official Gazette no. 406/2012. The law sets forth that all providers of public electronic communications networks and providers of electronic communications must retain all data concerned by the law, for a period of six months. Also, the providers must communicate such data, upon request, to the institutions in the national safety field. This information may be used for preventing and investigating serious crimes, for searching of missing persons, and for arrest proceedings.

The law transposes the provisions of Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

*Preparatory Colloquium Moscow (Russia), April 2013
Romania*

According to this regulation Article 22. - (1) Any intentional access, alteration or transfer of data retained under this law without authorization is a crime punishable by imprisonment of one to five years. (2) The attempt shall be punishable. Article 23. - Communication failure within the period stipulated in Art. 17 attract criminal liability under the law.

(D) Complementary optional information concerning law and practice (including statistics)

(1) Yes (Police, Prosecutor's Office, Courts of Justice)

(2) Yes, <http://www.efrauda.ro/>

(3) Yes.

(4) Computer fraud.

(5) Yes.

(6) Yes. The "Alexandru Ioan Cuza" Romanian Police Academy, Law Schools from the Universities and even master's programmes.

(7) Yes.

(8)

Forms and Means of Cyber crime	Frequently	Infrequently	Not occurred
Online identity theft (including phishing and online trafficking in false identity information)	x		
Hacking (including intrusion into computer systems; theft of information from computer systems)	x		
Malicious code (worms, viruses, malware and spyware)	x		
Illegal interception of computer data		x	
Online commission of intellectual property crimes		x	
Online trafficking in child pornography		x	
Intentional damage to computer systems or data		x	
Others		x	