

romanian cybercrime & computer crime legal blog

Romanian legal blog on cybercrime, cybersecurity, fight against cybercrime in Romania and worldwide. News, articles, cases, laws. This is the English version of the Criminalitate.info legal blog.

[Home](#)
[Romania: CYBERCRIME LAWS AND INSTITUTIONS](#)
[ABOUT US](#)

The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom. - Isaac Asimov, scientist and writer (1920-1992)

Sunday, February 9, 2014

Romanian Computer Crime provisions in the new Criminal Code (English Translation)

New cybercrime laws in Romania: As promised in the [previous article](#), we attempt a raw translation into the English language of the provisions regarding computer crimes and computer related crimes from the new Romanian Criminal Justice Code. **DISCLAIMER:** This is an unofficial translation intended purely for review purposes and not to be used directly in a court of law.

- Definitions - Prov. 181 and 182 define the meaning of Computer system, Computer data and Electronic payment instrument. Note that the new code does not provide also a definition for the notion of "without right", the way the old law did.

Art. 180 - Electronic payment instrument

An electronic payment instrument is a means for the owner to withdraw cash, recharge or discharge an electronic currency instrument as well as to transfer funds, other than those ordered and executed by financial institutions.

Art. 181 - Computer system and Computer data

(1) A computer system is any device or set of interconnected devices, or in functional relation, from which one or more devices ensure automatic processing of data, with the help of a computer program.

(2) Computer data means any representation of facts, information or concepts in a form which can be processed through a computer system.

- Title I - Offenses against the person
Chapter VI - crimes against personal freedom

Art. 208 - Harassment

(1) [...]

(2) Making phone calls or communications by means of distance communication, which by frequency or content causes fear to a person, shall be punished with imprisonment from 1 month to 3 months or a fine, if the act does not constitute a more serious offense.

(3) Criminal action is initiated upon prior complaint from the injured person.

- Title II - Offences against property
Chapter I - Theft

Art. 230 - Stealing with the purpose to use

(1) [...]

(2) With the same penalty in para. (1) is punishable the unlawful use of a communication terminal of another's or using a communication terminal connected without right to a network if there was a loss.

Chapter IV - Fraud committed through computer systems and electronic payment means

Art. 249 - Computer fraud

Entering, altering or deleting data, restricting access to such data or hindering in any way the operation of a computer system in order to obtain a benefit for himself or another, if it has caused damage to a person, is punishable by imprisonment for 2-7 years.

Art. 250 - Making fraudulent financial operations

(1) Making cash withdrawal operations, loading or unloading of an electronic money instrument or funds transfer instrument, using, without the consent of the owner, of an electronic payment instrument or identification data that allow its use, is punishable with imprisonment for 2-7 years.

(2) The same punishment is applicable to the operations referred to in para. (1), performed by means of unauthorized use of any identification information or by using false identification data.

Archive

▼ 2014 (3)

▼ February (3)

[Filing a criminal law complaint to the Romanian au...](#)

[Romanian Computer Crime provisions in the new Crim...](#)

[Updated Romanian Computer Crime Laws](#)

▶ 2010 (8)

▶ 2009 (1)

Need advice or assistance? Contact us:

contact@criminalitate.info

Categories

[00-All-articles](#) (12)

[01-Introductory-information](#) (2)

[03-Legislatie-romaneasca](#) (3)

[03-Romanian-laws](#) (2)

[05-Electronic-evidence](#) (3)

[07-Modus-operandi](#) (2)

[11-Practical-advice](#) (6)

[Events](#) (1)

[International](#) (1)

[Press](#) (1)

Search

Newsletter

Enter your email address:

Delivered by [FeedBurner](#)

Subscriptions

 [Posts](#) ▼

 [Comments](#) ▼

(3) Unauthorized transmission to another person of any identification data in order to perform one of the operations referred to in para. (1) shall be punished with imprisonment of one to five years.

Art. 251 - Accepting transactions made fraudulently

(1) Acceptance of a cash withdrawal operations, loading or unloading of an electronic money instrument or funds transfer instrument, knowing that it is carried out using a forged electronic payment instrument or used without the consent of the owner, shall be punished with imprisonment 1 to 5 years.

(2) The same punishment applies to accepting one of the operations referred to in para. (1), knowing that it was made through unauthorized use of any identification data, or by using false identification data.

Art. 252 - Sanctions for attempt

Attempted offenses under this chapter shall be punished.

- Title V - Offences related to corruption and service
Chapter. II Service offenses

Art. 302 - Violation of secrecy of correspondence

(1) Opening, theft, destruction or retention, without right of correspondence addressed to another, as well as disclosing without right the contents of such correspondence, even when it was sent open or was opened accidentally, shall be punished with imprisonment from 3 months to 1 year or a fine .

(2) Interception, without right, of a conversation or communication by telephone or by any electronic means of communication shall be punished with imprisonment from 6 months to 3 years or a fine.

(3) If the acts in para. (1) and (2) have been committed by a public official who has the legal obligation of professional secrecy and confidentiality of information to which it has access, the punishment is imprisonment from 1 to 5 years and interdiction of certain rights.

(4) The disclosure, dissemination, presentation or transmission to another person or to the public, without right, of the content of intercepted conversations or communications, even if the perpetrator was made aware of the contents by mistake or by accident, shall be punished with imprisonment from 3 months to 2 years or a fine.

(5) It is not considered a crime and shall not be prosecuted as a crime the above acts:

- a) if the author captures a crime or contributes to proving an offense;
- b) if the facts intercepted or disclosed are of public interest and have meaning for the community life and for which the public disclosure advantages outweigh the damage caused to the injured party.

(6) The possession or manufacturing , without right, of specific means of interception or recording of communications shall be punished with imprisonment from three months to two years or a fine.

(7) For the acts referred to in para. (1) Criminal proceedings shall be initiated upon prior complaint from the injured person.

- Title VI - Offences of forgery
Chapter. I - Forgery of coins, stamps or other values

Art. 311 - Forgery of debt securities or payment instruments

(1) Forgery of bonds, securities or instruments for making payments or of any other securities or similar, shall be punished with imprisonment for 2-7 years and deprivation of certain rights.

(2) If the act in para. (1) is done regarding an electronic payment instrument, the punishment is imprisonment from 3-10 years and deprivation of certain rights.

(3) The attempt is punishable.

Art. 313 - The circulation of counterfeit values

(1) The circulation of counterfeit securities referred to in art . 310-312 , as well as receiving , storing or transmitting them with the purpose to put into circulation, shall be punished with the punishment provided for the offense of forgery in which they were produced.

(2) The circulation of counterfeit securities referred to in art . 310-312, committed by the author or participant in the crime of forgery, is punishable with the punishment provided for the offense of forgery in which they were produced.

(3) Recirculation of one of the values provided in art . 310-312, by a person who discovered, after the entry into possession, that it is counterfeit, shall be punished with the punishment provided for the offense of falsification that were produced, of which special limits are reduced by half .

(4) The attempt is punishable.

In the news

[Romania cybercrime laws computer crime Romania computer fraud Romania](#)

[Suspected Online Hacker from Latvia](#)

SPAMfighter News (press release)

All three, including Calovskis, his accomplices a Russian individual Nikita Kuzmin, aged 25, and a Romanian person Mihai Ionut Paunescu, aged 28, faced accusation of executing one cyber-crime operation which thrust the Gozi malware. This virus ...

[Cybercriminals Target Bank Employees. Steal](#)

Dark Reading

KASPERSKY SECURITY ANALYST SUMMIT -- Cancun, Mexico -- An international cybercrime ring based out of Eastern Europe has pilfered some \$1 billion in two years from 100 different banks in nearly 30 countries using spearphishing emails targeting bank ...

[Related Articles »](#)

[Cybercriminals steal up to \\$1 billion from](#)

Daily Sabah

The company has been working with INTERPOL, Europol and authorities from different countries to uncover more details about the robbery, which is considered unusual because the cybercriminals targeted banks themselves rather than customers.

[eBay Works with Retailers to Crack Down on](#)

EcommerceBytes

"From Adversary to Trusted Partner" describes how eBay worked with retailers, credit card companies, and law enforcement to zero in on an estimated \$4.5 million to \$5.5 million in stolen retail goods in Florida in November in what was dubbed "Operation ...

powered by Google™

;))

--



Art. 314 - Possession of instruments for counterfeiting securities

(1) Manufacture, receipt, possession or transfer of tools and materials to serve in the forgery of values or securities referred to in art. 310, art. 311 para. (1) and art. 312 shall be punished with imprisonment of 1 to 5 years.

(2) Manufacture, receipt, possession or transfer of equipment, including hardware and software, in order to serve the forgery of electronic payment instruments, shall be punished with imprisonment for 2-7 years.

(3) No punishment shall be applied to the person which, after committing any of the acts referred to in para. (1) or paragraph (2) before their discovery and before the act of forgery was done, surrenders the tools and materials held, towards the judicial authorities or brings the existence of such tools to the knowledge of the authorities.

- Chapter. III - Forgery of documents

Art. 325 - Computer data forgery

The input, alteration or deletion, without right, of computer data, or restricting without right, the access to such data, resulting in inauthentic data, with the purpose to produce legal consequences, constitutes a crime punishable by imprisonment of 1 to 5 years.

- Title VII - Offences against public safety

- Chapter VI - Offences against the safety and integrity of information systems and data

Art. 360 - Illegal access to a computer system

(1) Access without right to a computer system shall be punished with imprisonment from 3 months to 3 years or a fine.

(2) The act in para. (1) committed in order to obtain computer data, shall be punished with imprisonment from 6 months to 5 years.

(3) If the act in para. (1) was committed on a system to which, through processes, devices or specialized programs, access is restricted or prohibited for certain categories of users, the punishment is imprisonment from 2-7 years.

Art. 361 - Illegal interception of computer data transmission

(1) interception without right, of a computer data transmission which is not public and is intended for a computer system, originates from such a computer system or is carried out within a computer system is punishable by imprisonment of 1 to 5 years.

(2) The same punishment applies to interception without right of electromagnetic emissions from a computer system that contains computer data which is not public information.

Art. 362 - Altering computer data integrity

Altering, deleting or damaging computer data or restricting access to this data without right, shall be punished with imprisonment of 1 to 5 years.

Art. 363 - Disruption of computer systems functioning

The act of seriously disrupting, without right, a computer system functioning, by inputting, transmitting, modifying, deleting or damaging data or by restricting access to data, shall be punished with imprisonment for 2-7 years.

Art. 364 - Unauthorized computer data transfer

Unauthorized transfer of data from a computer system or from a computer data storage means is punishable by imprisonment of 1 to 5 years.

Art. 365 - Illegal operations with devices or software

(1) Any person who, without right, produces, imports, distributes, or makes available in any form:

a) Devices or software designed or adapted for the purpose of committing any of the offenses referred to in Art. 360-364;

b) passwords, access codes or other such computer data allowing full or partial access to a computer system for the purpose of committing any of the offenses referred to in art. 360-364, shall be punished with imprisonment from 6 months to 3 years or a fine.

(2) Owning, without right, of a device, a software program, a password, access code or other data mentioned in para. (1) with the purpose of committing any of the offenses referred to in art. 360-364, shall be punished with imprisonment from 3 months to 2 years or a fine.

Art. 366 - Sanctions for attempt

Attempted offenses under this chapter shall be punished.

- Title VIII - Offences affecting the social life relationships
Chapter. I - Offences against public order

Art. 374 - Child Pornography

(1) The production, possession for display or distribution, purchase, storage, display, promotion, distribution and provision, in any manner, of child pornography is punishable by imprisonment from 1 year to 5 years.

(2) If the acts in para. (1) are committed through a computer system or other means of data storage, the punishment is imprisonment from 2-7 years.

(3) Accessing, without right, child pornography through computer systems or other means of electronic communication, shall be punished with imprisonment from 3 months to 3 years or a fine.

(4) child pornography means any material that shows a minor with an explicit sexual behavior or which, even if it does not represent a real person, simulates reliably, a minor with such behavior.

(5) The attempt is punishable .

- Title IX - Vote related offences

Art. 388 - Electronic vote fraud

Printing and using false access data, fraudulent access of electronic voting system or forgery by any means of the electronic vote ballots shall be punished with imprisonment of 1 to 5 years.

Art. 391 - Forgery of documents and voting related records

(1) Falsification by any means of the electoral documents from the polling stations shall be punished with imprisonment of 1 to 5 years and deprivation of certain rights.

(2) With the same punishment is sanctioned the enrollment of persons on the permanent voter list or on the supplementary voter list, of persons not belonging in this list.

(3) The introduction into use or the using of a computer program which alters the records or the results at polling stations or determines the illegal distribution of seats is punishable by imprisonment of 2-7 years and deprivation of certain rights.

(4) The same punishment shall apply to entry of data, information or procedures that lead to alterations in the national information system necessary to establishing the election results.

The original Romanian language provisions are available [here...](#)

Posted by ~cd at 10:00 PM 

 +2 Recommend this on Google

Labels: [00-All-articles](#), [03-Legislatie-romaneasca](#), [03-Romanian-laws](#)

No comments:

Post a Comment

Comment as: ▼

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

Awesome Inc. template. Powered by [Blogger](#).