Informatics Crime

CARMEN-SONIA DUŞE, DAN-MANIU DUŞE
"Lucian Blaga" University of Sibiu, Romania
Blvd. Victoriei no. 10, 550024 Sibiu
ROMANIA

MARCEL IOAN RUSU
Court of Law of Sibiu, Romania
Blvd. Victoriei no. 11, 550024 Sibiu
ROMANIA

Abstract: - The paper deals with the extent and characteristics of crimes committed in Romania in the area of informatics, information technology and communications, and especially with the manner in which the Romanian Law handles these types of crimes. Also, attention is paid to possible future approaches to improve the existing legal means.

Key-Words: Internet, legislation, Romania, informatics crime

1 Introduction

The technological achievement and the extremely rapid accession of informatics networks have lead to improvement of communication systems, developing contacts worldwide, the computers thus becoming indispensable instruments for carrying out different activities, with global impact on daily life, on carrying out businesses, communication or information management.

The emergence of the Internet facilitated by computers and interconnection techniques has radically changed the communication and informational exchange modality, the advantages of this one being multiple: accessibility, facility of usage, exclusivity, the possibilities of application in different fields of activity, distance independence. Internet thus appears not only as a simple assembly of hardware and software means that facilitates communication between computers [1] but also as a real structure and society [2] developing freely and openly.

It seems that the legislative provisions and international cooperation in this field did not keep up with the technological changes. Hence, the conclusion that a legislative background favorable to the development of informational society should be created and developed as well, at the same time with the inclination of modern society towards development of information technology.

The legislative harmonization within informational society [2] focuses on the protection of copyright, data confidentiality and anti-trust rules, promotion of technical standards that should ensure intercommunication between the new communication networks and multimedia development but prevent and fight informatics crime as well.

The explosion of informational techniques presents unquestionable advantages in the social economic life, but, at the same time, implies also phenomena outside the law [3].

Informatics crime represents a nowadays phenomenon, frequently reflected in mass-media. A study indicates even the fact that a stronger fear has emerged regarding informatics attacks and other ordinary frauds.

Informatics crime, the component of organized crime, is a real phenomenon in full expansion and the concrete modalities for preparing or committing such type of offence appear in diversified forms against which the possibilities to identify and establish culpability become more and more difficult. Due to this, it has been necessarily imposed the introduction in the Romanian legislation of special laws that should contain dispositions meant to ensure a firm response concretized in revealing, investigating and holding penally liable the perpetrators who commit such antisocial deeds [4].
In the Romanian doctrine, a distinction is made between legal crime, meaning all offences punished by trial courts, apparent crime that includes all crimes known by the police and the prosecution department and real crime, namely the offences known and unknown by the specialized state bodies which were committed in the social reality [5].

Informational crime is known only to a small extent by law enforcement agencies, therefore it is rather included in real crime, and consequently it is very difficult to provide an overview on the expansion and evolution of the phenomenon.

The increasingly larger access to data bases generated an increase in the degree of system vulnerability and offered at the same time the possibility to use them abusively or for illicit purposes, attacking traditional social values via computers and all together created the premises for producing significant damages to informatics systems and to data stored on these ones.

From the perspectives of article 17 of the Romanian Penal Code where the constitutive characteristics of the crime are presented, informatics crime represents the penal deed committed via the new informatics technologies that should determine a social danger, be committed by culpability and sanctioned by the penal law.

Informatics crime comprises the assembly of illegal activities performed by means of a computer, carried out via global electronic networks [6].

The most frequent infringements of the law are: economic espionage, identity theft, software piracy, usage of informatics viruses, credit card fraud, fraudulent electronic bids, goods and human trafficking or infantile pornography [7].

The facilities offered by advanced technique offer the possibility to easily exercise illicit activities outside the borders, informatics crime thus acquiring a transfrontier character, the problem of crime control being an international problem.

2 Favoring factors
During the year 2003, specialized services from Romania performed an activity of criminal investigation on 200 cases of which: 50% referred to fraudulent electronic bids, 30% to goods fraudulently ordered online, 10% dealt with unauthorized access to informatics systems and 10% referred to Nigerian letters, virus transmittal, infantile pornography, usage of false identity.

Lack of spectacular results in the fight against informatics crime consists in a series of objective and subjective causes, out of which we mention:
- sophisticated technology used by the offenders;
- lack of particular training of the officers within the law enforcement agencies;
- lack of a reaction plan in case of attacks by the victims of these criminal deeds, such circumstances may determine the impossibility to identify the damages caused;
- reluctance to report to the law enforcement agencies the perpetration of the crimes, etc.

Each cause, in its turn, has a motivation which, at first glance, may be justified. Some of the motivations for an omissive behavior to inform the law enforcement agencies would be: the concerns towards the public image that may be affected by the publicity around the action, the desire not to bear the costs for an eventual investigation, taking into account the complexity of such investigation; lack of possibility to recover the damages suffered even in the case when the offender is identified; lack of sophisticated equipments that may need high costs for the recognition of such offences.

On the other side, the training of specialized personnel implies a longer process with high costs and the carrying out of criminal investigation in this sector needs longer periods of time.

3 The legislative background in Romania
To the Romanian legislation, incrimination of such deeds injuring social relationships regarding the correct usage of the computer, assurance of confidentiality for data and information, preservation of public confidence in modern communication means, represented a necessary alignment to international normative standards.

There has not existed in Romania for a long time an express legal regulation for informatics crimes except for two laws: Law no. 16/1995 on protection of typographies and integrated circuits and Law no. 8/1996 on copyright and interfacing rights.

The classification of informatics crimes has been achieved only by Law no. 161/2003, which in Title III comprised:
- Section I – offences against confidentiality and integrity of data and informatics systems;
- Section II – informatics offences;
- Section III – infantile pornography through informatics systems.

The New Penal Code adopted by Law no. 301/2004, which was to be applied starting with July 30, 2005 and the applicability of this one has been prorogued until the month of September 2008, stipulates in Title X, “Offences against informatics data and systems” with two chapters:

1.) “Offences against confidentiality and integrity of informatics data and systems” art. 440 – 444, which implies:
- illegal access to an informatics system;
- illegal interception of an informatics data transmission;
- informatics data alteration;
- disturbance in the functioning of informatics systems;
- illegal operations with informatics devices or programs.

2.) “Informatics offences” art. 445 – 446, which implies:
- informatics counterfeit;
- informatics crime.

The Romanian criminal legislation incriminates this crime phenomenon by means of other offences as well, and from this perspective, of the role held by the informatics system in the process of committing the crime, these ones can be classified in the following way:

• offences committed with the help of informatics systems, in which these informatics systems constitute an instrument that helps to commit the crime such as:
  - “the offence of making the work public without any right” – art. 140 of Law no. 8/1996;
  - “the offence of reproducing a work without any right” - art. 142 of Law no. 8/1996;
  - “the offence of money laundering” – art. 23 of Law no. 21/1999;
  - “the offence of betrayal by transmitting secrets” – art. 157 Penal Code;
  - “the offence of revealing the secret endangering the security of the state” – art. 169 Penal Code and art. 12 of Law no. 51/1991, on national security;
  - “the offence of revealing the professional secret” – art. 196 Penal Code;
  - “the offence of fraudulent administration” – art. 214 Penal Code; „the offence of coin counterfeit or forgery of other values” – art. 282 Penal code;
  - “the offence of falsifying official instruments” – art. 286 Penal Code;
  - “the offence of material counterfeit in official records” – art. 288 Penal Code;
  - “the offence of revealing the economic secret” – art. 298 Penal Code;
  - “the offence of misappropriation” – art. 321 Penal Code;
  - “the offence of nationalistically chauvinist propaganda” - art. 317 Penal Code.

• offences committed by means of informatics systems, such as:
  - “offences against confidentiality and integrity of informatics data and systems” – art. 440 – 444 of the new Penal Code;
  - “informatics offences” – art. 445 – 446 New Penal Code;
  - ”offences of infantile pornography by means of informatics systems” – art. 18 of Law no. 678/2001 on preventing and fighting human trafficking and art. 12 of Law no. 196/2003 on preventing and fighting pornography.

4 Considerations for developing the fight against informatics crime

The informativeness of social life and usage by offenders of modern technologies have determined the gradual abandonment of traditionalist crime elements, the accent being placed on hiding the complex traces or consequences after perpetration of the deed .

The continuous progress in the field of informatics inevitably leads to risk growth and diversification of an external nature and consequently to the permanent change in the sociological profile of the informatics delinquent.

The new category of offenders who act in the cybernetic space comes from the most diverse environments, covering the entire social specter without any age limit.

At the level of Romanian society, the following future evolution in tendencies took shape:

- informatics offences become more and more frequent as long as the population is computer-dependent;
- nowadays, any person can virtually commit an offence within the informatics domain;
- it has been noticed that informatics crime exceeds the borders of the country, becoming international;
- the Internet becomes more and more like a “magnet” for organized crime.

Having in view those mentioned above, the assurance for information security is indispensable
to the normal protection of private life, of the secret of businesses and transactions, of intellectual property and of rule of law.

References: