NEW TECHNOLOGIES - NEW CRIMES

Ramona Mihaela COMAN[*]

ABSTRACT*: Technological development has seen a lot of progress, which has led to a considerable increase in efficiency in the most diverse domains of activity (economics, medicine, law, etc.); it has allowed transactions to be carried out very fast, the processing speed having increased considerably, thus enabling fast data storage and processing.*
The wider use of information technology and the Internet has radically transformed the world of economics, labor, education, research and administration. However, the accessibility and the widespread penetration of information and communication technologies, on the one hand, allow for a type of crime that would not be possible without computer systems, and on the other hand, it offers increased possibilities for committing "traditional" crimes. The legislator had to regulate new offenses or adapt the applicability of existing crimes to the virtual environment.

KEYWORDS: *New technologies; cybercrime; computer fraud*
JEL CODE: *K14, K40*

It can be unequivocally affirmed that the last 100 years will remain in history as the century of the computer, when technological developments have experienced the most progress in history. Beginning with the year of 1941 when Konrad Zuse, a German engineer considered to be a pioneer in the computer area, created Z3 - the first fully automated electronic computer with programmable functions based on binary numbers, the computer system has become an indispensable device for everyday life. The benefits that the computer has brought are indisputable, starting with the daily workplace support, reaching the medical system and ending with the vast computer systems that are used to defend national security. The informational revolution of the second half of the last century was the engine that led the current society to remarkable progress. The development of information technologies has considerably increased business efficiency in the most diverse spheres of activity (economy, medicine, law, etc.), telecommunication networks have allowed very fast transactions, the processing speed has increased considerably, and companies are able to store and process a lot of data.

The wider use of information technology and the Internet has radically transformed the world of economics, labor, education, research and administration. These instruments, which are important factors in the economic growth and competitiveness in various areas of global social and economic life, have been the subject of a careful analysis of the

[*] Lecturer PhD., University of Medicine, Pharmacy, Sciences and Techology of Tg. Mureș, ROMANIA.

European Union, which, in this respect, considered it important to adopt a new policy, largely oriented to the potential of new technologies.

This is all the more necessary if we consider the fact that that in the past decades the companies, which have invested heavily in technology, have also contributed greatly to GDP growth and to the development of occupational profiles.

But, in addition to the positive aspects of technological development, a number of negative phenomena have arisen - cybercrime, namely, direct or indirect, physical or logical actions, premeditated or unpremeditated, with the purpose of changing one or more conditions (confidentiality, integrity , accessibility) of an information system or subsystem. Accessibility and widespread penetration of information and communication technologies, on the one hand, allow for a type of crime that would not be possible without computer systems, and on the other hand, it offers increased possibilities for committing "traditional" crimes (Vasiu I, Vasiu L, 2005).

The exponential increase in connections and the number of users over the past years, as well as the high value of commercial transactions in the network, are concrete risk factors for computer aggression, which requires more and more sophisticated security measures. For example, increasing network connections and the use of electronic machineries and devices at home allow the so-called "computer pirates" to remotely disable alarm signals.

Therefore, due to the social danger created by these actions, it was necessary for the lawmaker to incriminate certain deeds, to provide for new offenses, thus entailing the most serious form of responsibility for antisocial deeds - criminal liability.

We need to make a distinction between "possibly" cyber-like crimes and computer crimes in a narrow sense. The possibly cyber-like crimes (or cybercrime in a broad sense) are those that can be committed also without using computer technology. For example, threats or blackmail through the internet. Cybercrimes in a narrow sense are those that involve computer or telematic systems, either as a material object or as a protected asset (Luberto, 2008). Thus, abusive access to a computer system, computer fraud, the spread of computer viruses, all these are examples of crimes that could not exist in a world without computers (Buonomo, 2003).

Regarding cybercrime, the doctrine considered that they could be divided into two categories: those committed by a programmer, called proprietary offenses, and those committed by anyone, common offenses (Resta, 1991).

Computer offenses can also be divided into: offenses that have been facilitated by information technologies and offenses where computers and computer networks are the target of the attack.

When a computer is used to commit a crime, records of fraud can be found on the data support and this includes information about the false identification, copy and distribution of information, intellectual property-subject information, the collection and distribution of information, and further more.

Crimes involving computers and computer networks as *objects* of crime usually consist in data and technical resources destruction. Attacks on information systems can be classified as follows (Lisi, Murano, & Nuzzolo, 2004):

- "individual", perpetrated by a single expert who often does not fully understand the consequences of his or her conduct. This is the case for a classical hacker who, in order to measure his own capabilities, "breaks into" a computer system.

- "organized", characterized by a precise *voluntas delinquendi* of a group of individuals who, even from different parts of the world, perform these activities against a computer system or a data bank for a specific interest of the group, for economic or political reasons.

This is the case of a computer frauds related to purchases / shopping based on certain information (identification number, code or password) specific for example to credit cards.

The most common *computer crimes* are the followings:[1] communication interception (sniffing), unauthorized access to computer and computer networks. This also includes the notion of hacking, network failure, the execution of "malicious software" that alters and destroys data and spoofing (usurpation of identity).

Computer attacks are not limited to these, but sometimes they are carried out to destroy information systems, taking the proportions of terrorist attacks. In order to fight against them, an effective criminal law framework is required, as well as an international cooperation against cyber terrorism in every Member State of the Union.[2] Therefore, along with the measures taken for the spread and technological development, it was also necessary to take measures against the illicit acts committed in this way.

Since 2001, the Council of Europe member states (with the help of Canada, the United States, Japan and South Africa - as observers) have drafted and signed the "Convention on Cybercrime". Subsequently, on 28 January 2003, the "Additional Protocol to the Convention on Cybercrime, on the criminalization of acts of racial and xenophobic nature committed through computer systems" was submitted to the Member States for approval. Romania also signed this Additional Protocol on 9 October, 2003.

The Convention and the Additional Protocol set the basic framework for the investigation and prosecution of computer-related crimes and for inter-state cooperation needed to stop this scourge. The Convention has brought to the forefront the need for criminal sanctioning of deeds such as: illegal access to a computer system, illegal interception of computer transmissions, computer forgery, computer fraud, child pornography on the Internet, violations of property rights and other related rights.

The chapter on international cooperation provided for a number of provisions on extradition (Article 24), legal assistance (Article 25), etc. With regard to international cooperation, Article 23 introduced three fundamental principles in the matter, namely: the parties must cooperate as much as possible with each other, cooperation must extend to all offenses relating to computer systems or computer data, cooperation must take into account the application of relevant international instruments relating to cooperation in criminal matters or agreements based on the uniform or reciprocal laws of each Member State domestic law.

---

[1] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach, 6 June,2001, COM (2001) 198 final.

[2] Idem

The Convention also stipulated in Article 12 the responsibility of legal persons and determined that each party should adopt the legislative and other measures necessary for the legal persons to be held accountable for acts stipulated in the Convention, committed on their own account by a natural person acting either individually or as a member of a governing body of the legal person.

In the Romanian legal system, the normative act that initially regulated the crimes in the computer area was Law 161/2003[3]regarding certain measures for ensuring the transparency and the exercise of the public dignities of public functions and in the business environment, corruption prevention and sanction, namely, Title III of Book I (Prevention and Combat of Cybercrime, Articles 34-67).

The facts incriminated by this law have been grouped into three categories, namely:

1. *Crimes against the confidentiality and integrity of data and computer systems* (e.g. unlawful access to a computer system (Article 42), interception, without right, of a non-public information transmission that is intended for a computer system, comes from such a system or is carried out within an information system (Article 43), the interception, without right, of an electromagnetic emission from a computer system carrying non-public computer data (Article 43 of the .2), the act of modifying, deleting or damaging computer data or of restricting access to such data without right (Article 44), etc.).

2. *Computer-related offences*, such as 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, the act of causing the loss of property to a person by the input, alteration of 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.

3. *Child pornography through computer systems*, which involves 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.

In order to ensure unity in the regulation of crimes, in 2009, the Romanian lawmaker considered it necessary to include in the content of the draft of the Criminal Code some of the crimes currently provided in special criminal law and which have a higher frequency in the judicial practice, including the computer crimes.

This introduced a new chapter that included patrimonial frauds committed through computer systems and electronic payment means. The texts resume without substantive amendments the provisions in the matter contained in the special laws. The penalties provided for these crimes have been correlated with the other sanctions provided for in the field of offenses against the patrimony, and it has also been taken into account the increased danger of these ways of committing these crimes. Also, the current criminal code has devoted a chapter to crimes against the security and integrity of computer systems and computer data.

As a matter of fact, we can see that the current criminal regulation in the field of new technologies crimes divides these into two broad categories: those affecting the patrimony (Computer Fraud, fraudulent financial operations, accepting fraudulent financial

[3] Published in the Official Gazette, no. 279/21 April, 2003

operations) and those who, irrespective of the infliction or not of a material damage to the patrimony of a person, are detrimental to cyber security (illegal access to a computer system, illegal interception of data transmission, alteration of computer data integrity, disruption of the operation of information systems, unauthorized transmission of data, illegal operations by means of computer devices or software).

At the same time, in some situations, the legislator provides for an aggravating form of a crime, when committed by means of a computer system. For example, in the case of child pornography, it is considered to be aggravating if the acts of production, exposure or distribution in any way, as well as possession for display or distribution of pornographic material with juveniles have been committed by a computer system or other means of storing computer data. The reasoning of the legislator was probably that, once spread in the virtual environment, these pornographic materials are hard to recover / destroyed and reach much faster for a large number of people. The consequences of the spread of pornographic material in this way are obviously much more damaging.

As far as cybercrime is concerned, the report for 2017[4] of the Directorate for Investigations of Organized Crime and Terrorism, which has the competence to conduct criminal investigations, indicates that in 2017 there were 1294 new cases of cyber crime, and 1701 cases have been resolved. As regards trends in cybercrime, they are similar to those registered at the international level, which are exposed in the IOCTA report (Internet Organized Crime Threat Assessment), Ransomware attacks being more and more frequent.

In addition to misappropriation of money transfer, interception of communications between traders, device abuse, and their remote control, cyber crime has seen new horizons through the use of Darknet in the illicit trade. Cryptocurrency is increasingly used by cybercriminals, and is now the main way of paying for Darknet operations.

Therefore, technology has allowed the creation of new ways of committing crimes, which are at the fingertips of young people. Thus, as an example, at the beginning of 2018, Targu Mures prosecution bodies identified the use of Darknet by young people to place online orders of high-risk drugs (Ecstasy pills) and their payment through the Bitcoin, the drugs being then delivered by courier from the Netherlands. This action meets the elements of the crime of introducing into the country high-risk drugs, a crime punished by the Romanian criminal law with 15-25 years of imprisonment.

REFERENCES

Buonomo, G. (2003). Le responsabilita penali. In T. E. Franceschelli V, *Comercio eletronico e servizi delle societa dell`informazione* (p. 324). Milano: Giuffre.

Lisi, F., Murano, G., & Nuzzolo, A. (2004). *I reati informatici. La disciplina penale nella società dell'informazione, profili procedurali.* Maggioli.

Luberto, M. (2008, March). I reati informatici contro il diritto alla privacz. La tutela fornita dal D.LG. N. 196 del 2003 e dal codice Penale. *Giurisprudenza di Merito* , pp. 898, 899.

Resta, S. (1991). *Elaborazioni informatiche e computer crimes.* Lecce, Mirella., p.100

Vasiu I, Vasiu L. (2005, January-March). Frauda informatica. (A. R. penale, Ed.) *Revista de drept penal* , p. 43.

[4] http://www.diicot.ro/images/documents/rapoarte_activitate/raport.2017.pdf