DOI:10.5281/zenodo.15075905

Cybercrime in Romania

Gheorghe Pîrcălabu

PhD Student, "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania,
Fully Admitted Lawyer, Bucharest Bar Association, geo.lexus@yahoo.com

Abstract: This study aims to provide a brief analysis of the criminal phenomenon in the field of software science. This phenomenon has grown, taking into consideration the fact that, lately, against the background of the lack of jobs and income for young people, the precarious economic situation in which the country has been struggling for 30 years, and the increasingly exacerbated technological development. Therefore, we believe that it is necessary to conduct a short analysis to define cybercrime succinctly but eloquently, outlining the causes and premises for the development of cybercrime, which could help to prevent, legislate, and penalize this criminal scourge.

Keywords: Cybercrime, Cyber Security, Law, Criminal Code, Cyber Fraud, Prevention, Investigation, Research

Introduction

The first attempt to define the term cybercrime was made by the Organization for Economic Cooperation and Development in 1983. After three years, in 1986, the experts of this organization defined the notion of "cybercrime" as "any illegal non-ethical or unauthorized behavior referring to an automatic data processing and/or data transmission" (International Telecommunication Union). Cybercrime in software field, generally called e-crime or cybercrime, one of the main manifestations of white-collar crimes, represents a criminal scourge which has experienced an impressive scale, development and adaptability in the last years in Romania. The teacher Tudor Amza, in his paper "Cybercrime", defined cybercrime as being "the act provided for by criminal law, committed with guilt by a person or a group of people who use a software and by means of communication of information by cable, they commit an act which presents a social danger that harms a person, a company or the interests of the state" (Amza and Amza, 2003, p. 54).

We can appreciate cybercrime, in a synthesized definition and much more current, as all the offenses committed through the software system, namely any criminal offense which involves an object or as a tool a software system, the criminal offense which usually aims to create a benefit to the offender by causing harm to the prejudiced people as a result of committing such offenses.

In order to better understand and know this phenomenon besides the definition of organized crime, we should know and understand other terms that are part of the usual vocabulary of this phenomenon. These terms include: *Software system* – "any device or set of interconnected or functional related devices, one or more of which provides for automatic processing of data by means of software" (Article 181 Romanian Criminal code, Law no. 286/2009), *Software data* – "any representation of facts, information or concepts in a form which can be processed by means of software system" (Article 181 Romanian Criminal Code), *Hacker* – "a person skilled in information technology who achieves goals by non-standard means" (Wikipedia) – software network breaker, software programs , cracker, *Phishing* – the transmission of false written emails or spams appears as if they had been sent by respectable banks or organizations, with the intention of luring the recipient to disclose important information, such as user names, passwords, account IDs, credit card PIN codes, *Identity theft, and Cloud.*

Causes and premises for the development of cybercrime phenomenon

We could say that the low standard of living, the increasing impoverishment of the population, the lack of jobs for young graduates and their inability to "accomplish" according to their studies and

training are identified as the first cause of the development of this criminal scourge. The criminals (unfortunately, most of them are young people with a degree of intelligence usually from the medium to the top) perceive this crime as an easy and quick way to get rich, in this context of the lack of means of existence at least at a decent level.

Another cause of the development of cybercrime is the naivety the negligence and even the indifference of the offended people. Most people are excessively naïve and gullible and out of the desire to catch an "extraordinary offer" or bargain "buy" all kinds of non-existent products or services at very low prices. Other people meet "their great love" via Internet and start sending money and gifts to criminals of common law in the name of love. Another contributing factor to the proliferation of this scourge can also be noted that a large number of people show a huge negligence in the use of software systems or electronic payment methods.

We could mention as premises for the development of cybercrime, the following:

- the lack of reaction of the offended people in the sense that they often do not report to the authorities;
- the development of technology in general and of software technology, in particular, and in this respect, we recall the fact that those who usually act in this criminal field are connected to and adapted to these technological developments and they are sometimes even one step ahead of the technology known by the ordinary citizen and even to the criminal investigation bodies and authorities;
- a coordinated, hierarchical, longevity and "well-established "criminal organization of criminals and the sophisticated technological means available to them;
- the lack of qualified personnel in the discovery, prevention and sanctioning of such acts or, in the happiest cases, of low specialized personnel or with poor training within the criminal investigation bodies;
- poor equipment or lack of techniques and necessary means for the detection and prevention of cybercrime at the level of authorized institutions, to do so;
- the lack of a reaction plan for different kinds of software offenses at the level of competent authorities;
- the software system, the virtual computing world has become more than a habit and we could even say a need in everyday life: we buy, we buy services, book goods and services, we transmit and spread information, write, read, socialize and fall in love in computing environment, and this thing makes us vulnerable to hackers, crackers and other software criminals that are specialized in phishing, skimming, fraudulent auctions etc;
- the vulnerability of computing systems;
- the cross-border nature of the majority of cybercrimes;
- the easy cover up of criminal traces by means of computing systems and some specially created programs;
- the possibility of moving and travelling of the offenders both in Romania and in other states makes them difficult to detect, pursue and prove;
- the continuous reorientation of the offenders in terms of cybercrime and the constant concern in the discovery of new operating modes and new software systems and software that can be compromised.

The detection of the causes and the premises for the development and perpetuation of cybercrime is absolutely necessary to establish policies, strategies and a plan to prevent and combat this criminal phenomenon (Franguloiu and Hegheș, 2023, p. 26-31).

Legislative provisions

The Romanian society, feeling the need to protect itself, regulate, penalize and combat such acts, has looked to regulating this criminal phenomenon from a legislative point of view. Therefore, building on existing international law (Convention on cybercrime - Council of Europe (2001) and

the Framework Decision of Council on May 28, 2001) and on the specific nature of software crimes committed on Romanian territory, two specific laws were initially adopted in this area: Law no. 365/2002, published in the Official Gazette of Romania, Part I, no. 483 of July 5, 2002, regarding electronic commerce and Law no. 161/2003, published in the Official Gazette of Romania, Part I, no. 483 of July 5, 2002 referring to measures for ensuring the transparency in the exercise of public dignity, public functions and in business field, the prevention and penalization of corruption, in Chapter III- "Prevention and combat of cybercrime". The legislator included and regulated these offenses in the New Criminal Code from the desire to create a single legislative framework, a uniform legislation and practice adapted to developments of this criminal scourge in 2014. The facts that are considered software crimes and penalized by the current legislation in Romania (the New Criminal Code and not only) are provided in: art. 208, art. 230, art. 249- 252, art. 302, art. 311-314, art. 324-325, art. 360-366, art. 374, art. 388, art. 391. These are part of the Romanian Penal Code, Law no. 286/2009, published in the Official Gazette of Romania no. 510 of July 24, 2009.

We point out that in the process of lawmaking and penalizing this criminal phenomenon, it should be specified and taken into account the fact that software crimes can be committed using the software systems, through software systems and/or on software systems.C IV of the Romanian Penal Code, Law no. 286/2009, published in the Official Gazette of Romania no. 510 of July 24, 2009, with subsequent amendments and additions, includes several crimes that represent fraud committed through computer systems and means of payment and here we list Computer Fraud in article 249, Carrying out fraudulent financial operations in article 250, Illegal operations with non-cash payment instruments in article 2501, Acceptance of financial operations carried out in article 251.

Of all these previously mentioned crimes, we chose to analyze the crime of computer fraud because this crime is most often committed by Romanian criminals in various forms and ways.

Brief analysis of the crime of computer fraud

The most common form of software crimes, in Romania, is the offense of CYBER FRAUD provided and penalized by Article 249 in Criminal Code Romanian – "the introduction, modification and deletion of software data, the restriction of the access to such data or the prevention in any way of the operation of a software system in order to obtain a material benefit to himself or another, if a person has been offended, he shall be penalized with prison from 2 to 7 years" (Article 249 Criminal code, Law no. 286/2009).

The special legal object is social relationships that protect a person's asset and the concrete use of software systems.

The material objective is modified, altered, introduced, deleted, restricted software data by which the material damage has occurred, the software systems which contains altered software data or which are prevented from functioning as a result of offender's activity.

An active subject could be any person.

A passive subject could be any individual or legal person who was really affected by actions on the software systems that he owns or uses.

The objective side.

The material element is the action of:

- introducing software data; or
- modifying software data; or
- deleting software data; or
- restricting access to software data; or
- preventing the operation of a software system in any way.

The purpose – the material acts of the offense of cyber fraud must be committed in order to obtain a material benefit for himself or another.

The subjective side is characterized by the intent that may be in the form of a direct or indirect intent.

There are opinions of some authors who consider that software fraud is always a premeditated act therefore the crime can only be committed with direct intent - the act can be committed only with direct intent, qualified by the intended purpose: that of obtaining a material benefit for himself or for another (Mihai coord., Ciuchi and Petrică, 2018, p.43).

The immediate follow-up – the crime of cyber fraud is a crime of result which means that it is consumed when damage or property damage occurs to the offended person.

The attempt is penalized.

The penalty – the offense of cyber fraud is penalized with imprisonment from 3 to 12 years.

Common types of cyber fraud

Fraud through online auctions consists of fraudulent auctions on websites specialized in online sales and purchases by fictitious posting for sale of cars, motorcycles and electronic equipment and other goods. Sellers either collect the money and no longer send the good or send a good with weak specifications, characteristics and very bad quality. Other times fraud through online auctions takes the form of the purchase of goods from the same sites specialized in sales purchases of goods and non-payment of goods.

Fraud involving investments, the offender sends an offer (usually by email) with the offer of an investment, a request for loans, on the sale of trips or other services at very low prices. The offended person transfers certain amounts of money and the offer will never be realized.

Fraud through social media sites in which the person-offender declares his “great love” towards the one he will take advantage of, then tells him/her that their love cannot be realized because he/she is sick or has a seriously ill relative and has to care of him/ her but has no money, sometimes tells the offended person that he/she would like to meet her/him but has no money to go, the victim sends the money but will never meet his “great love”.

Credit card fraud (identity theft) – card data are fraudulently used for online payment of various goods and services, on different sites that do not require additional authentication elements. In some cases, crackers manage to work at the “macro” level, breaking into sites that contain impressive databases with store customers, banks and so on, which obviously include the details of their credit/debit cards.

Software fraud by skimming – which involves the installation of some devices (wolf the mouth of the wolf, Citroen, etc.) on ATMs or POSs through which data are copied from the magnetic tapes of credit cards that are then used to rewrite new credit cards.

“Phishing” attacks - consist of the creation of fake websites that imitate the pages of public institutions or known private companies. The next step is to send e-mail messages to the potential clients of the institutions in question, with the aim of obtaining from them the confidential data. Practically, under a plausible reason (e.g. improvement of the security system, the existence of fraudulent transactions, etc.) confidential information is requested from the owner, the disclosure of which then allows the use of the instruments fraudulently. Links to fake pages are sometimes entered in the content of the messages, links are sometimes attached to messages.

Ways of fraud by requesting taxes - in this fraud scheme, the subject is asked to pay in advance a series of taxes, seeking to receive in return a large amount of money or certain prizes in objects. These fees are usually presented as processing fees, postal fees or fees for carrying out notarial deeds. The victim pays these taxes and gets nothing in the end.

Buying goods with counterfeit electronic payment instruments is also a common method.

Conclusions

After identifying the causes and premises of cybercrime, outlining the international and domestic legislation that regulates and penalizes this criminal phenomenon, analyzing the constituent elements of one of the most common crimes in the field of software science, and examining the various types and methods of committing software crimes, it becomes essential to propose methods, policies, and strategies to combat this growing threat.

Taking into account the fact that lately technology is found in all fields of activity and the company is dependent on technology, software systems and the online environment, it is imperative to establish software security policies and legal provisions that include and penalize any attempt to commit software crimes and problems of discovery, prevention and countering cybercrime including through the use of artificial intelligence (Franguloiu 2023, pp. 39-46). This leads to the emergence of the concept of cybersecurity, which can be defined as "that state of normality of digital information, resources and services provided by public or private entities in cyberspace". In concrete terms, cybersecurity can be achieved "by applying proactive and reactive security measures including security policies, standards and models, risk management and by implementing solutions for the protection of networks and information systems (Mihai coord., Ciuchi and Petrică, 2018, p.43).

The European Union has designed the Cyber Security Strategy 2016-2020 in this respect at the international level and at each country develops its own Cyber Security Strategy national level. As we have shown before in Romania, the cybercrime manifests itself in several forms: cyber-attacks (malware, ransom ware, DDoS attacks), software fraud (fictitious auctions of goods, compromise of user accounts on e-commerce sites or the creation of phishing sites for the collection of bank data) and fraud with bank cards (compromise of banknotes and the extraction of confidential information from customer cards).

Also, with regard to our country, we remember that Romania has adopted a Cyber Security Strategy, Law No. 362/2018 published in the Official Gazette of Romania no. 21 of January 9, 2019, on ensuring a high common level of security of networks and software systems and, in addition, the new criminal code and other special laws regulate and punish cybercrime.

As ways of discovering, preventing and countering organized crime we mention:

- the adoption of a legislative system adapted to the full range of crimes and activities that come into action of cybercrime, the creation of legislative levers that allow the prompt, in force and efficiency intervention of bodies with the attributes of prevention, investigation and research of cybercrime (Service for Combating Software Crime, a specialized structure within the Romanian Police)
- the cooperation at internal level between all authorities and institutions that have as their attributes of discovery, prevention and countering of organized crime and, the last, but not least, the cooperation between the public and private sectors in this field
- the international cooperation between states and between specialized authorities in the discovery, prevention and countering of organized crime
- the equipment and high-performance technology made available to all bodies and institutions with the powers of prevention, investigation and research of cybercrime
- high-performance cyber defense systems
- hiring highly specialized and professional personnel in the field within the institutions and bodies with the powers of prevention, investigation and research of cybercrime
- carrying out information and public awareness campaigns about the threats and risks that are present in cyberspace.

References

Amza T., & Amza C. P. (2003). *Computer Crime.* Lumina Lex.
Council of Europe. (2001). *Convention on Cybercrime.* (ETS No. 185).

Franguloiu, S., (2023). Principles for the use of artificial intelligence (AI) in the judiciary as derived from the European Ethics Charter. Justice efficiency and limitations, *Bulletin of Transilvania University Brasov,* Series VII: Social Sciences Law Vol. 16(65) No. 1 2023, pp. 39-46, https://doi.org/10.31926/but.ssl.2023.16.65.1

Franguloiu, S., & Hegheş, N.E., (2023). *EU-US Agreement on Combating Cybercrime*, Proceedings of the 34th International RAIS Conference on Social Sciences and Humanities, Washington DC, USA, The Scientific Press, Cambridge, MA, USA, p. 26-31, https://rais.education/wp-content/uploads/2023/12/RAIS-Conference-Proceedings-November_2023.pdf.

Law no. 161/2003, published in the Official Gazette of Romania, Part I, no. 483 of July 5, 2002.

Law no. 362/2018, published in the Official Gazette of Romania no. 21 of January 9, 2019, on ensuring a high common level of security of networks and information system.

Law no. 365/2002, published in the Official Gazette of Romania, Part I, no. 483 of July 5, 2002, regarding electronic commerce.

Mihai, I. C. (coord.), Ciuchi, C., & Petrică, G. M. (2018). *Current challenges in the field of cyber security – impact and Romania s contribution in the field,* The European Institute of Romania, Bucharest.

Romanian Criminal Code, Law no. 286/2009, published in the Official Gazette of Romania no. 510 of July 24, 2009, with subsequent amendments and additions.