Conferinţa internaţională de Criminalistică
Clasic şi modern în obţinerea şi valorificarea ştiinţifică a probatoriului
Cluj-Napoca, 13-15 iunie 2015

THE PROBLEM OF THE INVESTIGATION OF COMPUTER CRIMINALITY

Kornél GIRHINY[*]

Abstract. *As world changes, law enforcement forces have to face new challenges. One of these new challenges is obviously the scope of crimes, committed in digital space. We frequently come across with crimes, which neither have a scene, nor a witness, moreover, the personification of the delinquent is most likely an IP address.*

It is very hard, almost impossible to proceed an investigation with the devices of the classical criminalistics, regarding the deficiencies of the above mentioned criteria, therefore, criminalistics has to be refreshed, and the paradigm change is inevitable. Although, the process of such paradigm change started in the 90-ies, its improvement is rather slow, and criminalistics, in its present state, is unable to react properly for the emerging problems.

Being aware of such axioms, I reckon, that time has come to encounter such crimes on the basis of the same principles, even worldwide.

The objective of the present study is to introduce the problems, and to launch such a common sequence of ideas, which might contribute to the unified effort against the delinquents and the criminal organizations as well.

Keywords: *law enforcement, computer criminality,internet related crimes,cyber-space.*

1. Computer system, cure or blessing

Cybercrimes, parallel with increasing spread of computer usage, the penetration of large networks, the start of e-businesses and the growth of network information, are also equally developed. It has become worrisome not only for law enforcement but also for companies and individuals[1].

In the recent year in Hungary, these types of crimes are affecting a wider circle of people. Through computer networks not only the information needed for work, administration or entertainment find its way to the end user but also cyber criminals. The moral and material damage is significant for the internet service providers, however the internet user has also something to lose. By connecting to the internet they become potential victims. Thus, there's a strong need to find the solution to curb cybercrime as soon as possible.[2]

The goal of this study is primarily not to give an in depth and detailed explanation about this field and the connected investigations. My goal is to outline and present the issues and to get this over to a lot of potential victims and to propose a solution to solve the issues.

2. The expansion of the internet

The expansion of the internet created a new way for the offenders. By the 1990's, due to developments of computer networks the internet became available for the majority of people. Affected by this development more and more people had become a victim of the increasing number and kind of cybercrimes. The internet knows no boundaries, this is a well known fact for everybody by now. Thanks to this feature of the interne, the growing number of crimes needed immediate international cooperation.[3]

However the investigation of internet related crimes are not only differentiated only by its international feature. The loads of information make it impenetrable for the average people. Since cybercrimes do not require any personal contact, this makes it harder to find the perpetrator. The investigation of internet related crimes require special skills, in Hungary there isn't enough energy put into acquisition of this knowledge. The future goal is to train investigators so they can effectively solve these internet related crimes.[4]

One of the difficulties of preventing and effectively solving cybercrimes is, that they change rapidly It is difficult for the legislation to keep up with its development.

Computers were not affordable for the average person until the 1960's. However due to technical development and mass production computer prices dropped to its fraction to make it available for every household to have computers.[5]

Nowadays it's a known fact that there isn't only one computer in one household but everybody, even school children own their own device to get onto the internet. Since the internet is available for everybody, among its users appeared those, who, with their nativity and lack of knowledge can be a potential victims for internet related crimes.

To determine what exactly we mean by internet related crime is not simple.

The literature differentiate between the crimes and legal subjects, so differentiate between if the crime was committed with a computer (for example posting pornographic pictures of youth or children) or computer related crimes that are directed against computer systems or programs.[6]

3. Virtual space- cyber space

The so called information community is a heterogeneous group within the information society, its structure, operation is hard to understand. Practically this community shows the typical features of a society or group; however some scenes merge the same minded people regardless geographic boundaries. The interior space of this phenomenon is called virtual space or cyber space. The usage of the cyber or virtual indicator is still not clear exactly, they're used interchangeable frequently, however some specialists are reason for one or the other concept. If we approach the concept from a linguistic point of view, we can see that the Greek cyber word means boating or navigating, that implies moving and leading on the other hand the word virtual means apparent, imaginary[7], implying a sort of incomprehensibility.

A lot of people tried the concept of cyber or virtual space into words some of them I will introduce as an example.

The cyber space is a very complex phenomenon, which can be described as the 'conception space of the flow of information and communication which was created as the combination of the hardware of the digital world, computer software, telecommunication network and the human mind.' [8]

According to another interpretation ' the cyber space is a globally networked, computer maintained and computer generated, multi-dimensional, artificial, virtual reality. In this reality, where the computers are connected as windows, the seen and heard things are not physical, and not representing things, they are rather pure information appearing the form of character and action.'[9]

The exact definition is still not born, however there are elements of the concept, which are familiar terms, like:

a. Constantly changing and multi-meaning not physical, but still existing information and electronic space,

b. Location of the interaction between people and computers

The virtual space is considered a unique interior space of the information society; it's still hard to tell where to find this interior space. According to Matthew McNabb the cyber space 'is the place where the phone calls are being placed, or the faxed messages are between the fax machine and the destination.'[10]

4. Thoughts on computer related crimes

The possibilities given by computers and computer systems gave new opportunities to criminals or for even individuals with criminal intentions. This part of our society used these tools, systems to reach their goals and soon we became familiar with a new concept which is still hard to put our fingers on and has no clear boundaries, this is called cybercrimes.

One of these kinds of area is the criminal law. Within criminal law there are more known wording, as an example I will introduce some of them. The concept of computer related crimes is very wide, the computer is used as a tool to commit a very special crime according to the facts of traditional criminal law, and in a narrower sense these crimes are committed against computer system, programs and hurt the integrity of the computer system[11] .

According to Imre Kunos: ' Computer related crimes, is the group of crimes in which the information technology tools are used to commit the crimes'[12]

The suggested concept of CDIP of Brussels (Centre de Droit International Pénal):

'Information technology crime is every activity or failure in which in any computer system there's either material or intellectual harm is caused'.

As we can see from the above that there's not a solid concept for this field yet so like before I can only highlight the main characteristics, which are dominant in most concepts.

The main components of the concepts re the following:

a. committed by using or intruding computer systems or caused by computers,
b. the scene and the perpetrator is separated,
c. With the help of the Internet the perpetration can be international.

5. The basic problems of computer related crimes, the perpetrators and victims

The crimes committed in the IT space and the rest of the crimes are compared to each other from criminalistics point of view.

	Basic criminalistics questions	**Computer related crimes**	**Every kind of crimes, except for computer related crimes**
1.	What?	known	known
2.	Where?	not known, (not even country or continent) not always concludable	known, can be concluded
3.	When?	not known, can be manipulated	not known or known, can be concluded
4.	How?	not known, not always concludable	known or not known, can be concluded
5.	Who?	not known, usually only the tool known, and not always concludable	known, or not known, but can be concluded
6.	With whom?	not known, usually only the tool known, and not always concludable	known, or not known, but can be concluded
7.	Why?	known, or can be known after capture	known, or can be known after capture

The investigations of IT crimes are harder because of lacking the authorities still lacking the appropriate legal, knowledge or technology background.

The circumstances are for example there are no tangible traces present in the classical sense, communicating on computer networks provide some kind of anonymity to the perpetrator, the often take place in several states, the place of the crime is hard to establish, and the legal procedure is slower because of the cooperation procedure. It can be hard to even notice the crime and the victims might be against finding out certain facts if he or she keeps data on their computer that would cause economical damage to them if it gets found out.[13]

If we would like to describe this phenomenon systematically, these three marks we have to write about:

a. The latency. It can be states about crimes overall that there's a high rate of latency, it has more important points, frequently the victim themselves do not even notice that they become the victim of a crime or even when they notice very rarely they report this crime to the authorities.

b. The fastness. These types of crimes are prepared to be committed for a long time- although there are different modes also- the perpetration only takes a moment, the real time of the perpetration can be hardly timed.

c. The intellectual nature. The perpetrators are usually well prepared experts, and often are able to use computers and computer systems on an expert level.

I believe the solution could be to get computer user educated even within school education to get them to notice and prevent these kinds of expected emergencies.

With constant development it is inevitable that the investigating officers, judges, prosecutors are lacking knowledge, or they are only superficial since the technical development is moving at a rate that is very hard for them to follow properly. According to the law today that is not a requirement for police officers, prosecution or judges to get up to date information about the latest development of the computer world, but with that the question is surfacing if they are capable to make the right decision with lacking this kind of knowledge. To solve this issue they are now required to get an expert of the field, in my opinion is not the satisfactory solution since most of the times it is not even noticed that these experts might not have the right knowledge in the field of investigation. In my opinion the only solution for this matter could be the same that has been working in other countries so far, to educate some police officers, judges or prosecutors to get above the average IT knowledge.

The number of computer related crimes and their victims are showing a growing tendency. It is estimated that one million people become a victim of cybercrimes every day. The cost of computer related crimes can reach up to 388 billion dollars worldwide.[14]

It is also not an insignificant issue that there might be a conflict of interest between the criminal intent of the state and the people's individual freedom during the investigation. The other obstacles of investigation of these new kind of crimes are that the there's a significant delay in the legislation, since the earlier proceeding rules were matched to the norms of the physical world, and some of the rules are impossible to use in the virtual world.[15]

Due to the above mentioned difficulties the number and kind of obtainable evidences needed for the criminal liabilities is scarce and most of the time there are no other evidence than the digital ones for the reasonable suspicion.[16]

6. Relevance of being prepared

During the investigation of computer related crimes it can be concluded after investigating various situations that Hungarian Criminal Code doesn't require to punish preparatory criminal conduct, although this preparation behavior is very important during the investigation of the crime.

In the majority of the cases the preparation goes slowly, it is done systematically, it can take up to months or even years and that can connect the perpetrator to the crime. Creating a computer program or virus leaves a trace on the internet or any equipment they used. If during the investigation we can get the program that was used to commit the crime it can be traced down where it started. It's even worth to look for similar programs, the usually leave their typical sign on their inventions.

We also should never forget that basic fact that a computer is not only the typical device for cybercrimes, There are only a very few criminal offenses in the Hungarian Criminal Code which an IT tool couldn't be a tool and more often it is. Among them there are crimes that only the preparation is a crime by itself. The preparation of a murder or a terrorist act or not even mention a forging of public document, or preparing counterfeiting happens on a computer most of the time. These preparation act made only by using a computer device can become even finished. During the course of this investigation it is important to use the technical, tactical and methodical tools created for this type of investigation. The same is valid for the investigations are in progress for any other crimes, but for the preparation and execution of the crime a computer device or program was used or even if just an email was sent.

Computer science is actually a theorical and applied technology science that uses the tools of automated data processing and their various fields (such as building computers and their programming)

This includes the study of hardware and software and the operation assisting system of organizational, service and application features.[17]

IT tools by only using the internet can reach every other computer connected to the internet at the same time. This knowledge guides the perpetrators towards this field. Just by using their computers they can block, overload systems, data fishing, committing credit card fraud and the can almost accomplish anything on it. IT tools now include mobile phones, tablets, e-books and the development has just started. Nowadays our TVs or even our washing machines, refrigerator have their built in computer system. They can be programmed, can be accessed remotely, because of their built in memories they can also hold data.

Sometimes it can be hard to recognize an IT tool. For example pen drives and come in different shapes and sizes. The can be built into lighters, stuffed animals, little toys, jewelries, keys. During the house search an unknowledgeable officer can overlook this important evidence.

7. Planning and organizing the investigation

About the planning and organizing an investigation some officers often talk about them as they were each other's synonym that's why it's important to clear up the difference between them.

The planning of an investigation is based on the available data, taking the specific conditions and practical experience into consideration the determination of the investigation tasks and creating a program and notion for the fulfilment of them.[18]

Organizing the investigation is ensuring the conditions necessary for the planned tasks, the harmonization of the needs and possibilities.[19]

Investigation of computer related crimes are in many ways the same but also in many ways are completely different from other crimes. The average investigation tactics and methods can be used in this case, but because of the legal subject of the crime and the method of the perpetration, digital signs and digital evidences have to be handled differently, this requires a special knowledge. There aren't any uniformed textbooks or teaching aids for the recommendation of method of investigating cybercrimes. We have seen some descriptions and some case studies but more concrete, larger studies were not made in this subject yet. This has two reasons, one is that with a normal investigation we only give advice on a case by case basis there's no uniformed rule for every investigation, the other reason is that the with computer related crimes this is especially true.

There's only a very few people deals with modern criminalistics in Hungary. One of these few people is Csaba Fenyvesi's work is outstanding who sets a milestone in the field of modern criminalistics and the last piece of these milestones is the digital data itself.

The fact also makes it difficult with this investigation that the computer related crimes are only partially centralized, and practically according to the regulations the crime is under the control of the police authority where the crime occurred and until that his fact is not clear the crime is under the authority of the police station where the complaint was originally made.

As you can see from the above the investigating is not centralized, and even the professional leader activity isn't sufficient and it's even made further difficult by the domestic expert system, law.[20]

When a cybercrime happens usually there's only one complaint made for the investigating authorities, although we get to know the details of the crime, the attacked system, the aim and the result, the damage itself, but the collect the marks and collecting any other data is very rarely possible. Usually a previously occurred crime gets reported to the authorities, in which the marks and traces are usually gone or changed. Since the crime is committed in the cyber space, we can rely on virtual tracks. Hot pursuit on track is possible in theory, but in practice it's rare or not at all possible.

An immediate measure can be maybe the examinations and preservations of the computer data. This usually means the confiscation of the computer or its drive and the examination, interrogation by the expert investigator.[21]

There are like with every other statement of facts there are exceptions. There's a certain kind of cybercrime type, where there's a possibility of getting the direct data even if they part of an activity that can't be done right at the initial report of the crime. For example at a breach of copyright criminal offense where a hosting server is the part of the offense and that is where the documents are shared from. If after reporting a crime the server can be identified, it makes it possible to monitor the server's data for a while with an expert. In this case the expert puts a special tool into the servers communication system that can record every IP address the server get into connection with. This kind of method can only be used for a short period of time, since the speed of the server gets significantly reduced so the operator notices the problem pretty soon. The offenders of these kind of crimes are usually very qualified IT experts, the usually have some ideas about the investigating tools that the police officers use, so they can get suspicious easily. And if they suspect something as a defense they can destroy every valuable evidence that could've been used for the investigation. The data get deleted or make them unreachable.[22]

8. What is digital data?

Digital traces are created of the people in every moment of the everyday life. This only becomes digital evidence if the authorities start an investigation.

In the practical world the original digital evidence becomes a real, touchable object that is seized by the investigator, or with other restrictive measure keeps it in the original state. On the other hand these objects are geographically scattered- the cloud for example- when they can't be identified as the original meaning. This phenomenon is based on the property of the digital data, that the information content can be put together by the technology.[23]

The classification of the digital evidence has been already addressed by several authors. The most valuable is the theory of Tibor Peszleg for the practical point of view. The data he means by digital evidence are 'information in connection with a crime that have been stored, processed in some form on an IT device'.[24]

In his study Peszleg divides the evidences into three groups:

- Digital documents, 'that are simple documents, accounting data, pictures, videos, program or any other data that can be recorded by an IT device.'[29].

- In case of digital traces 'we are looking for temporarily recorded data that were created during the operation of an IT device, and average user doesn't know about it, but they are important for the operation of the system'.[29]

- Log data 'they are created during the operation and communication of whole systems. The part of them is logs that are created by law or economic rationality or they're created because of security requirements. This includes up and downloads of various log data, incoming and outgoing mails of mail server, registration data for emails, some network security programs, firewalls, log data intrusion signaling devices'[29].

By registration data Tibor Peszleg means the data that are created at a service provider if someone uses their services.

9. The 'choreography' of the investigation.

After examination of the report/ notification we try to find the possible existence of the crime, and if so, what kind of crime occurred. Unfortunately it happens a lot that the not fully prepared investigators get scared of the crimes committed over the internet and they try to direct the person reporting such crime to divert towards a different legal way or reject the report with some reason.

In an investigation against an unknown perpetrator it is hard to determine the direction of the investigation as the primary steps to be taken. There's a very few specific 'trace' above the report information. In this situation we can start from the data known by the usage of the internet. These kinds of 'traces' can be the IP address – later in details- the domain name and the email address. By the domain name we can check if the site contains illegal contents, date in connection with a crime (prohibited pornographic pictures for example). There are certain site in which by searching the domain name- centralops.net for example- we can find out who registered the given domain name, who operates it and with what service provider, who has the server that contains the website. With knowing that we can contact the organization.

If we know the email address, with the help of the above mentioned websites we can find out what organization we can look for. This way we can get the information given at registration, although those might not be valid. With web based email (freemail.hu for example) we can provide any information nobody will check on them. The service provider can give more information in this case, like what IP address was used at registration, from what IP address was used to log on last time or the time questioned, if there was a password change, what IP address that happened from and when that was. They can even provide the email list for authorities. It's important to mention that the content of the emails can be seen, for that and authorization is required from a judge.[25]

During the course of the investigation first we examine the information given with the initial report, check all the data, then we try to get by IP address, domain name or emails to identify individuals that we will interview. Among the means of proof the testimony has a major role. The injured person's testimony has the major role. The injured person has the most information regarding the object of the crime, they know the passwords, codes, the people with authorized access, the feature of the given computer system and the software used. It can be important the injured can provide information on the damage, that knowledge is important for the circumstances. The injured can provide the subject of the offense, the support of the existence of the criminal offense, mostly digital data. With the injured the individuals can be named as witnesses who also use or have access to it. The copyright infringing victims can also be used as witnesses and they can be the owner of the copyright (like performers, music producers, recorders, and radio and TV stations, filmmakers, and data base creators, publishers.)

The early part of the investigation of a crime we interview the suspects as a witness after finding the reasonable suspicion. The personal evidence has significance if the perpetrator planned to cover him and the computer used to commit the crime by using fake IP address and different kinds of computer defense systems so the computer couldn't be identified. In the case of computer related crimes, personal evidence is hard to collect and usually nobody else knows about the details of the crime.

It can happen that we confiscate the injured computer so we can examine the changes happened during the crime. Later during the investigation the suspected and other computers might be confiscated. It is very important that we get prepared for the house searches and the confiscation of the computers. If there aren't any computer experts on our team, we need to hire an expert of the field for the investigation to make sure to collect all of the date correctly. If it's not possible we have to confiscate the IT tool closed so it can be examined correctly later on.

It's typical that cybercrimes do not produce typical criminal clues. The digital clues that can be found sometimes carry very little data that it can pause the investigation. Most of the times only an IP address provided for the investigators, they can connect a person to the crime or if there's a person of interest there isn't any further data or personal evidence. Because of this with the majority of these crimes the perpetrator can't be identified, because of this the investigation gets suspended.

It is important of mention that the cybercrimes the place of the crime and the scene is where the perpetrator was located at the time of committing the crime and from where the command for the unauthorized access, change of data was given or where the profile was created or the breach of privacy right were committed.

It's an incorrect position that place of the crime is the physical location of the misuse of the data or computer in question. That was. This misconception might come for the presumption that on the computer misused contains the data that the crime was committed against and this is where the change in the data is taking place.

It's the characteristics of the IT management that a computer can be accessed from the other side of the world. The offenses controlled According to the Criminal Code are not punishing the *creation* of and *alteration* of the information but the act of making this happen, it punishes the behavior. The data manipulation, unauthorized access, obstruction of the function of the system can only happen by personal exposure. The punishable human behavior is unauthorized access, change or deletion of date, release of offensive data, and it is taken place where the perpetrator is physically located, where he is by the computer.

The investigation contains establishing the jurisdiction, the authority that is entitled to prosecute, the prosecution and the court.

10. Summary

Above – though job specifically still in general – mostly ideas for thought provoking characteristics and a little bit classical investigation features and the fusion of new type of cybercrimes showed up in this essay.

Based on the above written facts I believe that the computer related crimes will not stop, moreover with the further development and expansion of Information Technology these crimes will also expand further into the cyber space. In the mid and higher education the most desired major is computer technology and among our youth there is lot of highly educated information experts. Unfortunately it's my general experience that surely some of these well-educated young computer experts will use their knowledge illegal ways.

The system has to keep up the challenges. Although we do all we can do against crimes committed in the world of information technology, but we also see and have to admit that we are sometimes a step behind. We are not properly prepared to investigate complicated, international and to work together with international authorities.

It is necessary to improve the Hungarian law enforcement in this direction. We have to see that with other highly important crime interests we can't give any further advantage to the criminals committing cybercrimes.

We have to improve the professional and IT efficiency of the personnel, at least at every law enforcement territory has to have a team specialized in computer sciences, special IT tools have to be purchased and the special IT team has to be trained to be able to properly use them.

The economic aspects can't be an obstacle since there are more statements proving that hiring experts of the filed costs a lot more than this investment would altogether.

Right now the situating is not promising but because of that our everyday work is more dominant also in this field. There are more and more studies, international trainings and publications regarding cybercrimes, also the guidelines of international organization in the field so it is expected that soon the chief of the authorities will recognize the importance of this subject and they will make the much needed and inevitable changes and improvements.

Bibliography, internet sources

http://www.eurodetection.hu/szamitogepes_bcs.php

Dr. Pergel Józsefné: A számítógépes csalás és egyéb számítógépes bűncselekmények, Statisztikai Szemle, 79. évfolyam, 2001. 9. szám

Szentkuti Dániel - Szűts Márton: Az Internet és a büntetőjogi felelősség egyes kérdései *http://jesz.ajk.elte.hu/szentkuti15.html*

Bűncselekmények számítógépes környezetben: http://www.eurodetection.hu/szamitogepes_bcs.php

Számítógépes bűncselekmények - Cégvezetők Kiskönyvtára 2000/01. szám *http://cegvezetokklubja.hu/2000/01/szamitogepes-buncselekmenyek/*

Számítógépes bűncselekmények - Cégvezetők Kiskönyvtára 2000/01. szám *http://cegvezetokklubja.hu/2000/01/szamitogepes-buncselekmenyek/*

Bakos Ferenc: Idegen szavak és kifejezések szótára, Akadémiai Kiadó, Budapest, 1986;

Jakobi Ákos - *http://geogr.elte.hu/ref/REF_Cikkek/JakobiAkos/04_RTT13_fejezet3.pdf*

Benedikt, M. 1991). Benedikt, M.(1991) Cyberspace: Some proposals. In:Benedikt, M (ed.) Cyberspace: first steps. MIT Press, Cambridge, Mass., USA, pp. 119-124.

McNabb, M.(1998) „Personal communication" In:Carazo-Chandler, C.:Cyberspace– Another geography. Territories, Boundaries and Space. University of Canterbury,New Zealand.

Belovics Ervin - Molnár Gábor - Sinku Pál: Büntetőjog Különös Rész HVG-ORAC Budapest 2012.; p. 854.

Dr. Kunos Imre: A számítógépes bűnözés, Belügyi szemle 1999/11, p. 28.

Laczi B., A számítógépes környezetben elkövetett bűncselekmények nyomozásának és nyomozás felügyeletének speciális kérdései. Magyar Jog,12/2001. p. 727.

Európai Bizottság – Sajtóközlemény: A számítástechnikai bűnözés elleni küzdelem európai uniós központja az internetes bűnözők elleni küzdelem és az e-fogyasztók védelme érdekében. Brüsszel, 2012. március 28. *http://europa.eu/rapid/press-release_IP-12-317_hu.htm*

Parti K., Az internetes bűncselekmények nyomozásának egyes kérdései. Kriminológiai tanulmányok, 41. szám. 2004. p. 249

Szathmáry Zoltán: Bűnözés az információs társadalomban Budapest 2012: *http://doktori-iskola.ajk.pte.hu/files/tiny_mce/File/Vedes/Szathmary/Szathmary_nyilv_ertekezes.pdf* 2012. évi C. törvény a Büntető Törvénykönyvről *http://hu.wikipedia.org/wiki/Számítástechnika*

Lakatos János (szerk.) : Krimináltaktika I. Rejtjel, Budapest, 2004; 35. o.

ORFK Készenléti Rendőrség Nemzeti Nyomozó Iroda Korrupciós és Gazdasági Bűnözés Elleni Főosztály Csúcstechnológiai Bűnözés Elleni Osztály, illetve BRFK Korrupciós és Gazdasági Bűnözés Elleni Főosztály Gazdaságvédelmi Osztály I. Számítógépes Bűnözés Elleni Alosztály is készített

BRFK Korrupciós és Gazdasági Bűnözés Elleni Főosztály Gazdaságvédelmi Osztály I. Számítógépes Bűnözés Elleni Alosztály vezetőjének nyilatkozata alapján, saját kutatás keretein belül.

Máté István Zsolt: A digitális bizonyíték, *http://www.academia.edu/5105387/A_digitális_bizonyék_The_Digital_Evidence* (2014. 11.13.)

Fenyvesi Csaba: A kriminalisztika tendenciái. Budapest-Pécs, Dialóg Campus.2014. 62 o. 3/2008. (I. 16.) IRM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről 4. §a 2005. évi XLVII. tv. az igazságügyi szakértői tevékenységről.

BRFK Korrupciós és Gazdasági Bűnözés Elleni Főosztály Gazdaságvédelmi Osztály I. Számítógépes Bűnözés Elleni Alosztály vezetőjének nyilatkozata alapján, saját kutatás keretein belül.

Peszleg Tibor: Interneten, számítógépen történő nyomrögzítés, Ügyészek Lapja 12.évf. 1.sz., Ügyészek Országos Egyesülete, 2005.

1998 évi. XIX törvény a büntetőeljárásról

1994. évi XXXIV. törvény a Rendőrségről 69. § (1) *d)*

[*] *Police first lieutenant, instructor at the National University of Public Service, Faculty of Law Enforcement (Hungary); girhiny.kornel@uni-nke.hu.*

[1] *http://www.eurodetection.hu/szamitogepes_bcs.php*

[2] Dr. Pergel Józsefné: A számítógépes csalás és egyéb számítógépes bűncselekmények, Statisztikai Szemle, 79. évfolyam, 2001. 9. Szám.

[3] Szentkuti Dániel - Szűts Márton: Az Internet és a büntetőjogi felelősség egyes kérdései *http://jesz.ajk.elte.hu/szentkuti15.html*

[4] Bűncselekmények számítógépes környezetben: *http://www.eurodetection.hu/szamitogepes_bcs.php*

[5] Számítógépes bűncselekmények - Cégvezetők Kiskönyvtára 2000/01. szám *http://cegvezetokklubja.hu/2000/01/szamitogepes-buncselekmenyek/*

[6] Számítógépes bűncselekmények - Cégvezetők Kiskönyvtára 2000/01. szám *http://cegvezetokklubja.hu/2000/01/szamitogepes-buncselekmenyek/*

[7] Bakos Ferenc: Idegen szavak és kifejezések szótára, Akadémiai Kiadó, Budapest, 1986;

[8]Jakobi Ákos - *http://geogr.elte.hu/ref/REF_Cikkek/JakobiAkos/04_RTT13_fejezet3.pdf*

[9] Benedikt, M. 1991). Benedikt, M.(1991) Cyberspace: Some proposals. In:Benedikt, M (ed.) Cyberspace: first steps. MIT Press, Cambridge, Mass., USA, pp. 119-124.

[10] McNabb, M.(1998) „Personal communication" In:Carazo-Chandler, C.:Cyberspace– Another geography. Territories, Boundaries and Space. University of Canterbury,New Zealand.

[11] Belovics Ervin - Molnár Gábor - Sinku Pál: Büntetőjog Különös Rész HVG-ORAC Budapest 2012.; p. 854.

[12] Dr. Kunos Imre: A számítógépes bűnözés, Belügyi szemle 1999/11, p. 28.

[13] Laczi B., A számítógépes környezetben elkövetett bűncselekmények nyomozásának és nyomozás felügyeletének speciális kérdései. Magyar Jog,12/2001. p. 727.

[14] Európai Bizottság – Sajtóközlemény: A számítástechnikai bűnözés elleni küzdelem európai uniós központja az internetes bűnözők elleni küzdelem és az e-fogyasztók védelme érdekében. Brüsszel, 2012. március 28. *http://europa.eu/rapid/press-release_IP-12-317_hu.htm*

[15] Parti K., Az internetes bűncselekmények nyomozásának egyes kérdései. Kriminológiai tanulmányok, 41. szám. 2004. p. 249.

[16] Szathmáry Zoltán: Bűnözés az információs társadalomban Budapest 2012: *http://doktori-iskola.ajk.pte.hu/files/tiny_mce/File/Vedes/Szathmary/Szathmary_nyilv_ertekezes.pdf*

[17] *http://hu.wikipedia.org/wiki/Számítástechnika*

[18] Lakatos János (szerk.) : Kriminàltaktika I. Rejtjel, Budapest, 2004; 35. o.

[19] Lakatos János (szerk.) : Kriminàltaktika I. Rejtjel, Budapest, 2004; 35. o.

[20] 2005. évi XLVII. tv. az igazságügyi szakértői tevékenységről.

[21] BRFK Korrupciós és Gazdasági Bűnözés Elleni Főosztály Gazdaságvédelmi Osztály I. Számítógépes Bűnözés Elleni Alosztály vezetőjének nyilatkozata alapján, saját kutatás keretein belül.

[22] BRFK Korrupciós és Gazdasági Bűnözés Elleni Főosztály Gazdaságvédelmi Osztály I. Számítógépes Bűnözés Elleni Alosztály vezetőjének nyilatkozata alapján, saját kutatás keretein belül.

[23] Máté István Zsolt: A digitális bizonyíték, *http://www.academia.edu/5105387/A_digitális_bizonyék_The_Digital_Evidence* (2014. 11.13.)

[24] Peszleg Tibor: Interneten, számítógépen történő nyomrögzítés, Ügyészek Lapja 12.évf. 1.sz., Ügyészek Országos Egyesülete, 2005.

[25] 1994. évi XXXIV. törvény a Rendőrségről 69. § (1) *d)*