Research Article

Received: 5 June 2021 / Accepted: 15 July 2021 / Published: 5 September 2021

Collecting Evidence in Forensic Events and Comparison of the Digital Evidence Practices of Kosovo and Turkey

Dr. Mensur Morina

Hacettepe University,
Institute of Science,
Beytepe, Ankara, Turkey;
UBT University, Kosovo

Assoc. Prof. Dr. Endri Papajorgji

Dean, Faculty of Law,
Tirana Business University,
Albania

PhD. Muhammet Ali Eren

Hacettepe University,
Institute of Science, Beytepe,
Ankara, Turkey

DOI: https://doi.org/10.36941/ajis-2021-0122

Abstract

Evidence is an important concept in order to reveal whether a crime really exists or not and integrate it with all its elements. There are numerous methods of crime scene investigation in forensic cases. During the judgment phase, the most important factor that will help understand and decide the manner in which the incident took place is the evidence that will provide proof with regard to the incident. Therefore, evidence helps prosecutors and judges correctly understand and establish the relationship between the crime and the criminals and prove the committed crime and ensure correct, fair and rapid execution of the trial with the aim of reaching the material truth. Evidence obtained in the crime scene provides information with regard to the manner in which the crime was committed, the time of the crime, thebehaviour of the perpetrator, the suspect, the victim and the crime scene ensuring the establishment of the relationship between them. On the other hand, with the digital systems gaining more placein the life of the society, the crime scene has shifted from a physical environment to a digital one. Consequently, new types of crimes are committed digitally and as a result, the concept of digital evidence has arisen. There are no specific laws on the collection of digital evidence under Kosovo's legislation. On the other hand, there are legal regulations regarding digital evidence in exemplary countries such as Turkey. This study will comprise of the methods of gathering evidence in forensic cases and the comparison of the legal legislation on digital evidence in Kosovo and Turkey.

Keywords: *Criminal Procedure, Investigation, crime scene, criminal events, evidence, evidence collection methods, digital evidence, comparison of the laws of Kosovo and Turkey.*

1. Evidence in Criminal Procedure

In criminal proceedings, the main purpose of all government agencies participating in the trial is to obtain and collect evidence for the purpose of establishing the existence of a crime and its perpetrator. Government agencies have the objective as well as the legal obligation, to establish in a clear and fair manner whether a person suspected of a criminal offense has committed that criminal offenseby providing evidence.

In fulfilling their functions defined by the current legislation, with particular emphasis on the provisions of KCPC, the criminal justice institutions shall determine whether the crime was committed, identify the offender who committed the crime, and clarify all other conditions related to the appropriate determination of the degree of guilt and the social danger posed by the criminal to the environment in which he lives. A criminal offense is an event that has occurred in the past and is tried in court. The circumstances of the criminal offense (with all of its details) and the guilt of the defendant can only be determined with evidence.

In case of a criminal offense, in addition to the violation of the guaranteed legal rights, there is also violation of the order that the community and the statemust protect. By fulfilling its duty to protect legal rights, the state must act against the perpetrators of criminal offenses and restore the broken order. Therefore, in criminal procedures, criminal sanctions can be imposed and applied against the person who committed the criminal offense. Therefore, in order to impose the correct criminal sanctions in accordance with the conditions foreseen in the Criminal Code with the purpose of achieving the objective of the criminal procedure while also paying attention to not punish the party that is not guilty, the real offender shall, under the framework of the criminal procedure, be given the correct criminal sanction by proving the important evidence (Sahiti, 2016).

As part of the investigation of a criminal offense, it is the responsibility of government agencies, such as the Police and the State Prosecutor's Office, to investigate, collect and submit evidence to establish the guilt or innocence of a suspect.

The legal obligation of the state authorities involved in the proceedings for the determination of the facts in an accurate and complete mannerprior to making a legal decision is determined in paragraph 1 of Article 7 of the KCPC. The court, the state prosecutor and the police participating in criminal proceedings must truthfully and completely establish the facts which are important to rendering a lawful decision.[1]

This procedural legal provision lays down the grounds and fundamental limitations of the state bodies that are obliged to make their decisions only after establishing the facts. These facts can only be determined after handling and analysing the evidence that corroborates the concrete facts. This legal limitation represents the principle of material truth which is one of the fundamental principles in criminal procedure.

The above provision requires maximum commitment from the police, the state prosecutorand the court in order to establish the facts in the concrete criminal case, and these authorities should be careful in analysing and evaluating these facts, especially prior to rendering any judgment decision. This attention should be particularly high in the early stages of the judgment when rendering decisions that restrict human rights and freedoms (Hajdari, 2016).

In addition, the state prosecutor and the police participating in the criminal proceedings have a duty to examine carefully and with maximum professional devotion and to establish with equal attention the facts against the defendant as well as those in his or her favour, and to make available to the defence all the facts and pieces of evidence, which are in favour of the defendant, before the beginning of and during the proceedings.[2]

Another legal limitation with regard to evidence specifically referring to the prosecutor is the

[1] *Kosovo Criminal Procedure Code, Article 7, paragraph 1.*
[2] *Kosovo Criminal Procedure Code, Article 7, paragraph 2.*

obligation of the prosecutor to consider inculpatory as well as exculpatory evidence and facts during the investigation of criminal offences and to ensure that the investigation is carried out with full respect for the rights of the defendant and that evidence is not collected in breach of Chapter XVI of the present Code. (This part of the Criminal Procedure Code of Kosovo clearly sets out the manner of obtaining evidence in criminal proceedings).[3]

The role of the police in obtaining evidence in investigation procedures is of high importance. In many countries of the world, the police are the main body conducting criminal investigations and depending on the structural organization police, state prosecutor, court etc run these procedures. However, the police themselves have officials/detectives with basic as well as advanced criminal investigation knowledge. Depending on the type of crime allegedly committed, the police always engage qualified and trained investigators to investigate this incident with the aim of identifying the perpetrator.

After the police officers are engaged tocollect evidence, a clearer idea will emerge as to whether there are doubts with regard to the existence of criminal elements and potentially a perpetrator. Once sufficient evidence regarding a committed crime and the existence of one or more persons are potential perpetrators is collected, the Police, after cooperating with the prosecutor, prepare a criminal report and thereafter, in accordance with the assessment of the prosecutor, continue with other procedures, including investigations, additional evidence collection or the investigation can be enhanced by requiring other individuals to be included in the investigation. Should these prosecutorial investigations turn out to be positive, and in cases where one or more persons are suspected, there is sufficient evidence that a crime has been committed, the prosecutor's office, as a responsible state body, shall open the indictment and send it to the competent court.

Police officers, in addition to the large number of proceedings usually set out in various legal and sub-legal regulations, also have some specific legal powers to collect material evidence and handle the same in a professional manner. The police shall carefully collect the evidence and preserve it in the appropriate manner that permits the evidence to be tested by the competent laboratory.[4]

Thus, it was clearly established that the constitutional authority for the collection of material evidence from the scene is the police who, with high professionalism, have to seek, collect and present material evidence. In addition, after taking the material evidence, it is very important that the evidence found at the scene is sent to authorized laboratories for adequate analysis and comparison, by applying appropriate methods and techniques to ensure adequate packaging and handling with high professionalism.

Where the police and prosecution have met their legal obligations with regard to the evidence, often the case is sent to court. The trial takes place in the competent court, and in this case the main purpose of the prosecution body is to prove that a particular person has committed the crime.

The role of the defence during the trial is to challenge the evidence presented by the prosecution and, if there is new evidence, to convince the court that the defendant has not committed a criminal offense or that the defendant has no criminal liability in terms of the crime for which he was charged. As an independent body, after considering the evidence, the court will make a judgment based on the merits and render this decision on the guilt or innocence of the defendant on the basis of the evidence presented to it or the evidence formally obtained.

The court has a legal obligation to deal with the weight of each evidence separately and together, to ensure that evidence is obtained in accordance with the legal provisions, and that such evidence can convincingly prove a person's guilt or innocence,

Every court decision is based on evidence, thus the court's role in evaluating the evidence is crucial. The court must never base its decision on unlawful evidence and never render a decision in the absence of evidence. The main purpose of the court is to make a judgment based on the merits,

[3]*Kosovo Criminal Procedure Code, Article 48.*
[4]*Kosovo Criminal Procedure Code, Article 71, paragraph 1.*

with full legal support, based solely on evidence obtained in a legal manner.

The criminal procedure legislation prescribes court procedures, meaning that court decisions must solely be grounded on evidence provided and received in accordance with the law. In accordance with KCPC, the court must render its decisions solely on the basis of legal evidence to be examined and dealt with during the trial. The court renders its decision on the basis of the evidence examined and verified in the main trial.[5]

Any evidence (in terms of its accuracy and relevance) that underlies the court decision must be analysed and evaluated at the hearing. Naturally, the compatibility or contradiction of these evidence will be looked at, and the same will be compared with each other prior to the court deciding on this matter (Hajdari, 2016).

Evidence obtained before the main trial and ultimately revealed in the main trial must be examined and verified at this stage of the proceedings before the court reaches a specific decision. This approach stems from the requirement that those involved in criminal proceedings are aware of the evidence regarding the case and are able to give concrete statements regarding them, especially for those whose obligations and interests are affected by the court's decision-making mechanism (Hajdari, 2016).

In any legal system, it is a widely accepted standard for a court to base its decisions on acceptable and legal evidence. Any state aiming to have an efficient, professional and impartial judicial system strives to ensure that court decisions are only evidence-based and are under no circumstances affected by other external factors.

A criminal act or offense is usually an event that occurred a long time ago, and legislatures together with judicial authorities are obliged to identify and prosecute this illegal act. This determination should be made with evidence that reveals decisive facts regarding the manner in which the crime was committed and the person responsible for it.

Altogether, every trial process must be conducted and concluded on the basis of evidence, and evidence must be obtained in accordance with legal provisionsno matter what. Because every other transaction or any evidence obtained through illegal means will,in most cases, be unacceptable regardless of whether the evidence clearly and accurately demonstrates an important fact. Legislators have imposed strict procedural restrictions for the purpose of avoiding tendency to abuse state institutions that could obtain evidence in criminal proceedings in an illegal manner in the name of law enforcement. While this legal restriction forces government agencies to be vigilant and accountable, it also guarantees that nobody will be charged or punished for illegal evidence.

The court cannot base its decision on inadmissible evidence. Therefore, in accordance with paragraph 2 of Article 258 of the KCPC, the court may prohibit taking evidence in the following cases:

1. If the taking of such evidence to supplement other evidence is unnecessary or is superfluous because the matter is common knowledge;
2. If the fact to be proven is irrelevant to the decision or has already been proven;
3. If the evidence is wholly inappropriate, impossible or unobtainable; or;
4. If the application is made to prolong the proceedings. Inadmissible evidence is regarded as essentially any information without support, based on rumors and evidence or information deemed impossible or unreliable at first glance, and without known origins.[6]

2. Digital Evidence

Technical and technological developments recorded in recent years, with particular emphasis on the last two decades, have had a huge impact on the daily lives of people. The invention and use of many technical devices, especially information technology, has led to their tremendous use in various areas

[5] *Kosovo Criminal Procedure Code, Article 8, paragraph 2.*
[6] *Doracaku i Provimit te Jurisprudences. (2016) 235.*

of social life.

New IT assets and programs have found use in all areas of life, in national and international transport, the financial and banking system; science, culture, sports, manufacturing and many other areas affecting daily life.

The use of these devices and programs has definitely made life easier and more dynamic; however, on the other hand, there is a need to set rules and restrictions on the use of new technology, as IT devices can, of course, in addition to good intentions, be used for malicious purposes, respectively, to perform certain illegal actions.

The use of computers and international information networks in the modern world has resulted in fundamental changes in business and human life. Obtaining data transport that previously required hard work and a long time to gather and organize for a person is now easier. Personal, institutional computers, education, research and study centres have provided great convenience and benefits. Today it is almost impossible to organize, plan and implement many research projects without the use of computer technology. The application of the computer gave a great impetus to the advancement of science and the well-being of humanity. However, its wide application in daily life has led to some detrimental phenomena that do not favour the development and well-being of contemporary society (Halili, 2016).

Therefore, each state is required, under its own legislation, to identify key aspects regarding the use of various IT disclosures, with particular emphasis on those that may be used by certain individuals for illegal gain. Global changes that have led to advancementsin IT have revealed other high-risk areas where each state should consider the organization of the best legal protection, as the damage in cases of criminal offenses through the use of IT devices and programs is enormous and unimaginable ranging from those affecting the lives of people to material damage, violation of human rights and freedoms, privacy, etc.

The innovations that the development of information technologies (IT) brought to our lives, our citizens and various institutions have been subjected to a very dangerous crime problem since these technological developments are not used only for good purposes. This situation has prompted not only certain countries but also various regional and world organizations to act rapidly to ensure securityin the use of IT innovations. The world is in need of legal protection in cyberspace more than ever.

Known as one of the types of crime with high social, the abuse of technology by criminal elements is known as 'cybercrime', where it can appear as computer fraud, computer forgery, breach of security systems, or any form in which the computer system is involved as a networked tool and represents the action of a person in a computer system. Computer crimes are defined as follows: 'Criminal offences against individuals or groups of individuals by causing financial gain, damage to the image of the victim, or direct or indirect physical or mental harm using modern technology'. In daily practice, there are two types of behaviours observed in cybercrime (Shkembi, 2015).

Criminology is an old social phenomenon; however, as I mentioned above, a new type of crime is emerging in the field of IT. The change brought about by the computer revolution is the automation of every process by transforming each informationinto a binary code, processing and generating new information. The computer revolution has brought with it the further complexity of criminal behaviour, the integration of computer systems into existing technologies, and anyone in this technology could be massively harmed. Based on various types of crime in advanced contemporary societies, a new type of crime is evident in the field of cybernetics (Halili, 2008).

Scientifically, cybercrime is considered to be — criminal offenses committed against individuals or groups of individuals for the purpose of monetary gain, damage to the image of the victim or causing physical or mental harm directly or indirectly using modern technology or otherwise defined as the commission of actions through a command system, where the purpose is to profit through fraud, breach of security systems, exploitation, etc. (Shkembi, 2015).

Cybercrime is manifested in a variety of manners; mostly fraud, piracy, program theft, program intrusion, private software intrusion and the detection of private intimate secrets, various other

manipulations, political and industrial espionage, and many other forms of criminal activity (Halili, 2008).

Considering the interdisciplinary nature of cyber law, the topic of digital evidence pertains to a wide range of legal practice areas such as criminal law, criminal procedure law, and civil procedure law.[7]

It is possible to define digital/electronic evidence as "information and data that are stored on an electronic device or transmitted through these tools that have an investigation value" (Özen & Özocak, 2015, 134). In other words, it is all kinds of digital information that has to be understood from electronic evidence, which can be produced, converted and saved in digital format and become perceptible with the help of Information Technology (IT) systems (Savić, 2020). This information and data mainly consist of notations consisting of 0 and 1 and are not perceptible by the sense organs. It is possible for them to become perceptible by sense organs if they are transferred with various software (Warken, 2017). In this sense, it is stated that forensic informatics carries out expert witness activities in terms of criminal investigation and prosecution, where the activity of evaluating the evidence is carried out by the judicial authority (Duran, 2019).

In order to have successful protection against cybercrime, the Republic of Kosovo has adopted legislation that is currently considered adequate to prevent and combat such crimes.

The Criminal Code of the Republic of Kosovo, foresees only one criminal offense of this nature under its Article 327 "Access to Computer Systems". The definition in paragraph 1 of this Article states as follows: Whoever, without authorization and with the intent to obtain an unlawful material benefit for himself, herself or another person or to cause damage to another person, alters, publishes, deletes, suppresses or destroys computer data or programs or in any other way intrudes into a computer system shall be punished by a fine and imprisonment of up to three (3) years.[8]

This legal provision also provides that, in case of illegal access to computer systems that cause material damage or benefits in amounts of more than ten thousand (10000) euros, the same shall be considered a serious form of committing this crime. Paragraph 1 of this Article states that if the offense provided for in paragraph 1. of this Article results in a material benefit exceeding ten thousand (10,000) EUR, or material damage exceeding ten thousand (10,000) EUR, the perpetrator shall be punished by a fine and imprisonment of six (6) months to five (5) years.[9]

Being aware that this legal provision alone is not enough to prevent and combat cybercrime, Kosovo's legislatorshave enacted a special law for this field, adapting it to international conventions, best practices of developed countries and the level of technological developments in Kosovo as well as beyond. This was the Law No. 03/1-166 on Prevention and Fightof the Cyber Crime.

According to the Law on Prevention and Fight of the Cyber Crime, this law aims at preventing and fightingcybercrimes with concrete legal measures, by providing adherence to human rights and protection of personal data, preventing, detecting and sanctioning violations through computer systems. The purpose of this law is to prevent criminal acts in this area and successfully identify the offenders and perpetrators of these acts, and the ultimate aim is to impose sanctions on all individuals who commit crimes of this nature.

In addition, this law specifies, in a more precise manner, which actions are considered to be crimes, and gives more precise explanations with regard to the elements of criminal offenses, their mode of functioning, criminal sanctions and other necessary data. More precisely, they are prescribed as criminal acts against confidentiality, integrity and availability of the computer systems data; Unauthorized interception; Unauthorized transfer; Hindrance of computer systems operation; Unauthorized production, possession and attempt; Computer related criminal acts; Causing loss of

[7]*Cemal Araalan Digital Evidence in Turkish Law, GSI Articletter, Part 15, P. 207.*
[8]*Criminal Code of the Republic of Kosovo, Article 327, paragraph 1, Intrusion into Computer Systems.*
[9]*Criminal Code of the Republic of Kosovo, Article 327, paragraph 2, Intrusion into Computer Systems.*

asset; Child pornography through computer systems.[10]

The Law on Prevention and Fight of the Cyber Crime also stipulates actions of state bodies related to the investigation of these crimes, which are more procedural in nature and must be implemented during the conduct of investigations. Pursuant to this law, it is very important thatwe provide some basic definitions of statements related to this crime area in this study. These definitions are as follows:

- Cybercrime - a criminal activity carried out in a network that has as objective or as a way of carrying out the crime, misuse of computer systems and computer data.
- Computer system - any device or device assembly interconnected or under an operative linkage, of which, one or more provide automatic data that are processed through computer programs.
- Automatic data processing - a process by which the data are processed to the computer system through computer programs.
- Computer program - a group of instructions that may be implemented through a computer system in order to achieve certain results.
- Computer data - any representation of facts, information or concepts in such a form that could be processed by means of computer systems. This category involves any computer program that may initiate computer systems to perform certain functions.
- Service provider - any natural or legal person that provides an opportunity to users to communicate by computer system, and the person processing or collecting data for these providers of services and for users of services provided by them.
- Data on the traffic - computer data concerning the communication that through a computer system and its output, representing part of the communication chain, indicating the origin of the communication, destination, line, time, date, size, volume and time duration as well as type of service used for communication.
- Data on users - any information that may lead to identification of the user, including type of communication and service used, address of the post office, geographic address, IP address, telephone number or any other number of access and means of payment for pertinent services as well as any other information that may lead to identification of the user.
- Security measures - refer to utilization of certain procedures, means or specialized computer program by means of which access to the computer system is limited or forbidden to a given category of users.
- Pornographic materials of minors - refer to any material that presents a minor or an adult shown as minor of an explicit sexual behaviour or images which, although it does not present a real person, simulates, in such credible way a minor with explicit sexual behaviour.
- Interception - obtaining, illegal seizure of the data from unauthorized persons.[11]

As in other countries around the world, the Republic of Kosovo, possesses a strategy for the prevention of cybercrime among state and institutional mechanisms, including other laws that can be applied to the successful development of this state activity. In addition to the above-mentioned laws (Criminal Code and Law on the Prevention and Fight of Cyber Crime), the following laws also apply to this area:

- Constitution of the Republic of Kosovo;
- Law No. 03/L-050 on the Establishment of the Kosovo Security Council;
- Law No. 03/L–166 on Prevention and Fight of the Cyber Crime;
- Law No. 04/L-145 on Information Society Government Bodies;
- Law No. 04/L-094 on the Information Society Services;

[10] *Law on Prevention and Fight of the Cyber Crime, Articles 9-16.*
[11] *Law on Prevention and Fight of Cyber Crime, Article 3 - Definitions.*

- Law No. 04/L-109 on Electronic Communications;
- Law No. 05/L-030 on Interception of Electronic Communications;
- Law No. 03/L-172 on the Protection of Personal Data;
- Law No. 04/L-076 on Police;
- Law No. 03/L-142 on Public Peace and Order;
- Law No. 03/L-063 on the Kosovo Intelligence Agency;
- Law No. 04/L-149 on Execution of Penal Sanctions;
- Law No. 04/L-065 on Copyright and Related Rights;
- Law No. 03/L-183 on Implementation of International Sanctions;
- Law No. 04/L-213 on International Legal Cooperation in Criminal Matters;
- Law No. 04/L-052 on International Agreements;
- Law No. 04/L-072 on State Border Control and Surveillance;
- Law No. 04/L-093 on Banks, Microfinance Institutions, and Non-Bank Financial Institutions;
- Law No. 04/L-064 of the Kosovo Agency on Forensic;
- Law No. 04/L-198 on the Trade of Strategic Goods;
- Law No. 04/L–004 Private Security Services;
- Law No. 03/L-046 on the Kosovo Security Force;
- Code No. 03/L-109 on Customs and Excise;
- Law No. 04/L-099 on Amending and Supplementing Customs and Excise Code in Kosovo No. 03/L-109;
- Law No. 03/L-178 on Classification of Information and Security Clearances;
- Criminal Code of the Republic of Kosovo No. 04/L-082;
- Criminal No. 04/L-123 Procedure code;
- Law No. 03/L-122 on Foreign Services of the Republic of Kosovo;
- Code No. 03/L-193 on Juvenile Justice;
- Regulation No. 18/2011 on the Distribution and Transfer of Classified Information.12

3. The State of Digital Evidence in the Turkish Criminal Procedure Law No.5271

The main purpose of the Turkish Criminal Procedure Law and the main law that expresses it is to reach the truth without causing human rights violations (Öztürk, 2010). One of the protection measures resulting from interference with fundamental rights and freedoms is; It is a "judicial search" measure, which refers to the search process carried out in people's residences, other enclosed places, on top and their belongings, with the aim of catching the hiding suspect or accused, detecting the evidence of the crime and seizing the goods subject to confiscation, upon the emergence of a crime (Nurullah, Feridun and Ayşe, 2006). There is also a regulation regarding the collection of digital evidence in the Turkish criminal procedure law. Article 134 of the Criminal Procedure Code (CPC), the search, copy and seizure measures on computers, computer programs and registers is regulated under the title. This protection measure regulated in Article 134 of the CMK constitutes a special form of the "search" and "seizure" protection measures regulated in Articles 116 and 123 of the CPC. According to this[13];

1. In the investigation conducted for a crime, if there are strong reasons for suspicion based on concrete evidence and if there is no possibility to obtain evidence in any other manner, the judge or where delays are not allowed the state prosecutor will issue a decision for the

[12] *National Cyber Security Strategy of the Republic of Kosovo. (2016-2020) 18.*
[13] *https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf.*

search of computers and computer programs and computer logs used by the suspect, make copies from the computer records, and decipher the records and prepare them in text form. Decisions made by the state prosecutor are submitted for the judge's approval within twenty-four hours. The judge makes a decision within twenty-four hours at the latest. In case the deadline expires or a negative decision by the judge, the copies made and the texts decipheredshall be immediately destroyed.

2. If the computer, computer programs and computer logs cannot be accessed due to the inability to decipher or the hidden information cannot be accessed or the process will take a long time, these tools and equipment may be seized in order to ensure a solution and make the necessary copies. If the password is cracked and the necessary copies are made, the confiscated devices will be returned without delay.
3. During the process of seizing computer or computer logs, all data in the system shall be backed up.
4. A copy shall be made from the backup taken in accordance with the third paragraph and the same shall be given to the suspect or his/her attorney, and this issue shall be recorded in the minutes and shall be signed.
5. It is possible to copy all or some of the data in the system without having to seize the computer or computer logs. The copied data shall be printed on paper, this issue shall be recorded in the minutes and signed by the parties concerned.

The following results can be achieved as a result of the interpretation of the relevant Article of the Law.

Search in computer data is a special form of general search (CMK 116 et al.), and seizure of computer data is a special form of general seizure (CMK 123 et al.), in order to obtain electronic evidence, taking into account the characteristics specific to digital evidence (Hüsnü , 2018).

While the subject of general search and seizure is concrete traces, findings and things inside the building or on the person, what is at issue here is abstract electronic data on various devices such as computers (Özbek, Doğan and Bacaksız, 2019). In accordance with the aforementioned qualifications of digital evidence, the fact that the search and seizure measure in computer data is arranged in a special way meets this need (Çekiç, 2021).

Since the right to personal information belonging to the individual is a fundamental human right, it is clear that legal regulation will be required to restrict the right. In addition, this procedure must be carried out with a decision of the judge.

In terms of discovering the truth, there is no doubt that the records on the computers will constitute evidence, traces, pieces and signs in criminal and civil cases. To this end, searches in computer programs and files have been subjected to certain conditions in order to provide this opportunity and to keep individual benefits preserved.

In this regard, as is known, there was no clear regulation on search and seizure, search on computers. To this end, the guarantee of a judge is accepted in Article 134, even if it is to protect the rights and freedoms of an individual.

Electronic data is highly dynamic. It can be easily corrupted, changed, deleted. Unlike printed documents, electronic data can change even without human will. Records kept in information systems, automatically updated log files, and files with automatic backups are changed independently of people. Actions such as operating a closed computer, turning off an open computer, scanning files, copying them to another location change many data. The officer who intervenes in the system can delete and corrupt many data without his knowledge and intention.

Evidence is confidential in nature. They are not directly visible. Appropriate hardware and software are needed to see and make sense of the data. A computer, a word processor program, a screen and a printer are needed in order to see and understand the data produced by the word processing program. The data can only be understood when it is opened on the computer with a word processor program and viewed on the screen or printed out. The printout printed on the paper

will not fully reflect the data, the meta-data will not be visible. It is a great deficiency to make an evaluation by being content with screen and printouts (Değirmenci, 2014). However General search carried out inside the building or on a person in order to obtain evidence of crime, physical activities performed with the five senses such as palpating, scanning with eyes, looking at secret places, smelling, hearing to find something concrete.[14]

In order to decrease theinterfere with personal privacy, this Article stipulates that the suspect's computer should be searched first. For example, seeingif only unlicensed software is installed on a computer, to see if only one user has been identified on a computer, or to see if there are 5-10 image files containing child pornography in existing files on a computer, all of these actions can be carried out swiftly at the scene without seizing the computer. In this case, the searches should be made with forensic information methods without altering the original data of the computer.

Searches can be carried out in multiple ways: The search is carried out at the scene and the printouts are printed on paper and signed as a report, the search is carried out at the scene and the printouts are prepared electronically, copies from the computer are taken at the scene and the search is carried out later or the computers are seized at the scene and the operations are carried out in offices.

However, in cases where there is more than one computer at the scene, if the data fields on the computers are large, if detailed searches are to be made on deleted, hidden and encrypted files, the devices must then be seized.

Computers have a structure that allows them to be easily changed and have parts due to their structure. As a result of this feature, in some cases, it may be necessary to immediately seize computers, computer programs, computer networks, remote computers and data storage units.

If the computer, computer programs, computer networks, remote computers and data storage units under examination belong to a large company and the company is unable to continue its activities upon seizure of devices, or if the data to be seized is a part of the data in the whole system, copies of them as a whole or part of them can be seized without seizing all systems. This issue shall also be recorded in the minutes and signed by the relevant persons.

If the systems are to be seized and the suspect request it, a copy of this backup shall be made and given to the suspect or his attorney, and this matter shall be recorded in the report and signed.

As a result, according to the Turkish Criminal Procedure Law No.5271, if there is no possibility to obtain evidence in any other way during an investigation carried out for a crime, the judge, upon the request of the public prosecutor, decides that the computer and computer programs used by the suspect shall be searched, copies made from the computer records, and these records shall be deciphered and converted into text. If the computer, computer programs and computer logs cannot be accessed due to the inability to crack the password or if the hidden information cannot be accessed, these tools and equipment may be seized in order to make a solution and make the necessary copies.

4. Conclusion

Numerical evidence is the data obtained from the information systems used to determine the action in criminal procedure. Since it is included in data information systems that will be the subject of digital evidence, it is necessary to define the process from information systems until it is brought before the judge. As a matter of fact, digital evidence is a concept that should be approached with care as a form of evidence.

The technical process from obtaining digital evidence to its submission to the court must also include methodologies used in the field of forensic informatics. There are problems that can be

[14] *Regulation on Judicial and Prevention Searches, Official Gazette publication date 01.06.2005, Issue number 25832.*

encountered in obtaining digital evidence depending on the development of technology.

The first stage of the forensic informatics process, which includes the whole process from the moment digital evidence is first obtained to the reporting process and presented to the court, is the stage of collecting and preserving the digital evidence. This stage includes the period of time when the probability of corruption of andigital evidence, which is an important element in the resolution of the incident and being used in a crime committed, is the highest. Because, preserving the integrity and validity of andigital evidence, which is subject to wrong persons and wrong transactions when it is first obtained, carries a great risk and this causes question marks in the later stages of the judgment. In this respect, complying with the basic principles to be followed during the collection of digital evidence, performing the necessary live analysis, image acquisition, determination of the hash value, taking the time stamp, ensuring the protection chain and packaging the obtained digital data, carrying and storing it is of great importance in terms of the safety of the investigation and prosecution process.

Digital evidence has been approached technologically and legally within the framework of Article 134 of the criminal procedure law, which is the primary safeguard measure in Turkish law. It should be taken into consideration that obtaining numerical evidence is a legal protection measure and the relation of the said protection measure with fundamental rights and freedoms should not be ignored. Since there is no regulation on digital evidence in Kosovo, it would be appropriate to draft a regulation on digital evidence for the Kosovo Law, similar to Turkish Law. However, if such a regulation on digital evidence is not drafted, certain issues regarding fundamental rights and freedoms shall be guaranteed under the Constitution of Kosovo. Rights protected in digital evidence search should be considered from all aspects. Firstly, a regulation on the manner of collecting digital evidence by the law enforcement in Kosovo should be regulated in a manner that is in compliance with the constitution and legislation of Kosovo. In other words, the process starting from the collection of evidence to the submission of the evidence to the state prosecutor, and from the state prosecutorto the court and evaluation at the court should be regulated.

As a result, whether there is a regulation on digital evidence or not, the matter here will be the protection of the fundamental rights of the perpetrator and victim.

5. Acknowledgement

This article is produced from the doctoral thesis of Hacettepe University, Institute of Sciences.

References

Araalan, C. (2015). Digital Evidence in Turkish Law, GSI Articletter, Part 15, p. 207.
Çekiç, B. (2021). Bilgisayar verilerinde arama, kopyalama, el koyma tedbirinin hukuki niteliği ve benzer kavramlar, Namık Kemal University Faculty of Law Journal, 155-188.
Değirmenci, O. (2014). Numerical (Digital) Evidence in Criminal Procedure, 1st Edn, Seçkin Publications.
Duran, G. Y. (2019). Searching, Copying and Seizure in Computers, Computer Programs and Logs, in the Code of Criminal Procedure (CMK), Başkent University Faculty of Law Journal, Vol. 14, P. 173-174, p. 203.
Hajdari, A. (2016). Komentari i Kodit te Procedures Penale te Kosoves. Prishtina.
Halili, R. (2016). 'Kriminologji. Prishtina.
Hüsnü, A. (2018). Forensic Prevention, Search and Seizure, page 179, 1st edn, Adalet Publications.
Nurullah, K. Feridun, Y. and Ayşe, N. (2006). Criminal Procedure Law as a Branch of Procedural Law, Istanbul Arıkan Publications.
Özbek, V. Ö. Doğan, K. Bacaksız, P. (2019). Criminal Procedure Law, 12th Edn, Seçkin Publications.
Öztürk, B. (2010). The Code of Criminal Procedure. Istanbul.
Özen, M. Özocak, G. (2015). Legal Regime of Forensic Informatics, Electronic Evidence and Search and Seizure of Computers (CMK art. 134), p. 59.
Sahiti, E., Murati, R. (2016). E drejta e procedures penale. Prishtina.
Savić, L. I. (2020). Die digitale Dimension des Stafprozessrechts, Berlin 2020, p. 43.
Shkembi, A. (2015). Harmonization of Albanian and European Legislation'. Tirana.

Warken, C. (2017). Elektronische Beweismittel im Strafprozessrecht-eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 2, NZWiST 2017, 329.

Legislation

Kosovo Criminal Procedure Code.
Kosovo Doracaku i Provimit te Jurisprudences (2016). Pristina.
Kosovo Law on Prevention and Fight of Cyber Crime.
Kosovo National Cyber Security Strategy. (2016-2020). Prishtina.
Regulation on Judicial and Prevention Searches, Official Gazette publication date 01.06.2005, Issue number 25832.