E-ISSN 2410-8693
ISSN 2410-3918

Academic Journal of Business, Administration Law and Social Sciences

Vol. 10 No. 2
July, 2024

sciendo

Research Article

© 2024 Elsa Miha & Iris Pekmezi
This is an open access article licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (https://creativecommons.org/licenses/by-nc/4.0/)

Electronic evidence in the criminal process

Elsa Miha
Prosecutor at Prosecutor's Office of the Judicial District of Tirana

Iris Pekmezi
Head of Legal Department, One Communication Company

DOI: https://doi.org/10.2478/ajbals-2024-0010

Abstract

In a criminal process, the evidence constitutes one of the most important components of the burden of proof. In today's reality, where technological devices and information technology are undergoing an unstoppable development, electronic evidence in the criminal process is increasingly reflecting a great practical importance, which directly affects not only the investigation and trial of criminal offenses in the field of cybernetics, but also in the discovery of all criminal offenses provided for in the Criminal Code of the Republic of Albania.
Unlike the classic evidence provided expressly and in detail by the criminal procedural law, the provision in this legislation of electronic evidence is special, borrowed almost completely from the content of the Budapest Convention and which has as a distinguishing characteristic a generalizing provision and at the same time is open to include a wide range of evidence, in the variety of electronic evidence.
However, despite this good forecast, due to the characteristics of electronic evidence, the lack of individuals who have specialized knowledge for obtaining and securing them, with the ultimate goal of using them in the criminal process of evidence, remains a challenge.
Thus, with the focus on creating a clear picture about electronic evidence in the criminal process, this manuscript will analyse the current legal provision of electronic evidence in Albania, the efficiency of this provision i
n practice, including identifying characteristics of electronic evidence, the principles of electronic evidence, as well as the process of obtaining and securing them as usable during the criminal process.

Keywords: Evidence, electronic evidence, criminal offense, Budapest Convention.

1. Introduction

The Code of Criminal Procedure of the Republic of Albania is the law that has the

duty to ensure a fair, equal and regular legal proceeding to protect personal freedoms and the rights and legitimate interests of citizens, to help strengthen the legal order and implementation of the Constitution and state laws.[1] This law was approved for the first time in 1995 and was amended over the years in accordance with the needs of the current Albanian criminal procedure (Miha, 2024). Referring to duties, its fair implementation reflects great importance for every subject of the criminal process, including the court, the prosecution, the judicial police officer, the defendant, the lawyer of the defendant, the victim and the accusing victim in a criminal process.
Especially related to crimes in the field of cybernetics, criminal procedural law is of particular interest to be studied due to the existence of electronic evidence.
Thus, "*Complete and effective legislation that meets the requirements of human rights and the rule of law is the basis for criminal justice measures against cybercrime and the use of electronic evidence in criminal proceedings. This is particularly true of the specific procedural law powers available under the Budapest Convention, as a comprehensive domestic criminal law framework for these powers also facilitates international cooperation on cybercrime and electronic evidence with other Parties to the Convention. Clear concepts of electronic evidence, categories of data and precise limits and conditions for procedural powers are essential in this respect. Therefore, the adoption of comprehensive and effective legislation on cybercrime and electronic evidence that meets the requirements of human rights and the rule of law is considered a strategic priority*."[2]
In this sense the definition of electronic evidence, its legal provision, principles and best practices regarding the handling of electronic evidence with the aim of its admissibility in judicial procedures, sources of electronic evidence, some general considerations of classic, traditional and digital forensic medicine, as well as the legal mechanisms of the European Union in the function of electronic evidence will be analysed.

2. Evidence in a criminal trial

As it is mentioned, our procedural system is the accusatory one, in the content of which its basic principles are sanctioned. It is based on the dialectical method of truth, which means proving an event started from a thesis, which is the charge brought to life by the prosecution body, comparing it with another opposing thesis, which is the defence thesis, that lead us to a synthesis that is the judicial decision. This is the way to reach the judicial truth, which as the final stage of a criminal process, reflects a special importance both for the effects it brings immediately, and the effects it brings in society.
Thus, solving a criminal case means performing a series of procedural actions, as a result of which, proving the circumstances of the event, leads the court to the truth. The realization of this basic purpose for the criminal procedure requires certain legal

[1] Article 1, Criminal Procedure Code.
[2] Evaluation report on the taking and use of electronic evidence in criminal proceedings under national legislation in South Eastern Europe and Turkey, accessible at the link: https://rm.coe.int/3156-52-electronic-evidence-report-v4- alb/16808cfd36 .

facts to be proved, the proof of which is realized through evidence.
Specifically, the word *"proof"* comes from Latin and is the root of the word " *approvattio"*, which means approval. In the context of criminal law, by the notion of " *evidence"* we must understand a data that contains the accuracy of a fact. Meanwhile, referring to the provisions of the Code of Criminal Procedure, by the term evidence we must understand *"... notifications on the facts and circumstances related to the criminal offense, which are obtained from the sources provided for in the criminal procedural law, in accordance with certain rules by him and that serve to prove whether or not the criminal offense was committed, the consequences resulting from it, the guilt or innocence of the defendant and the degree of his responsibility"*(Article 140 Criminal Procedure Code). Due to the special character and often considered delicate in terms of respect for basic human rights and freedoms and the various violations that can be committed during the criminal process, with or without intention by the subjects, the types of evidence and the methods of their receipt is provided for in the Code of Criminal Procedure and specifically from Article 153 to Article 226 (Miha, 2024).
As it emerges from the wording of Article 149 of the Code of Criminal Procedure, evidence according to our legislation constitutes the essential phase of proof and its very meaning is closely related to the criminal offense. This comes from its definition as "*... notification on the facts and circumstances related to the criminal offense".* The definition of evidence is not exhaustive in the sense of expressly defining each of the evidences. However, the fact that they must "*... be obtained from the sources provided for in the criminal procedural law in accordance with the rules defined by it" is exhaustive.* This is a formal criterion of evidence, a consequence of the general criterion of law and criminal law in particular.
Following the analysis of this provision, in the function of this article, it must be brought to attention another provision of the criminal procedural law,[3] through which it should be understood that the evidence in a criminal process has no limit. They are endless in types and ways; it is enough that during their acquisition they have not violated basic human rights and freedoms. This forecast came for the first time in 2017, a year which brought substantial procedural changes, which were aimed at sanctioning effective norms that resisted the changes of time, especially those of a technological and computer nature.
Thus, in order to have the quality of evidence, notifications on the fact, sources of knowledge, data must be obtained from one of the sources provided for in the Code of Criminal Procedure and in accordance with the rules determined there according to the principle "*jura novit curia*", the principle of the legality of the evidence. Also, the evidence must serve to prove the commission or non-commitment of the criminal offense, its consequences, guilt or innocence and the degree of responsibility. This is related to the meaning of evidence and circumstances related to the criminal offense.

[3] Article 8/a, Criminal Procedure Code. States that: "*1. The facts in the criminal process are proven with any evidence, provided that they do not infringe the fundamental human rights and freedoms. 2. The prosecuting body must collect and examine both the evidence that incriminates the defendant and those that are in his favour".*

In case the evidence does not prove the fact, and a fact related to the criminal offense, it cannot have the value of the evidence.

3. Electronic evidence in a criminal trial

Based on the above, it can be stated that electronic evidence originates from electronic tools such as computers and their peripheral devices, computer networks, mobile phones, digital cameras and other portable devices (including data storage devices), as well as from the internet. They are no different from traditional evidence, in that the party presenting them in the legal process must be able to demonstrate that they reflect the same circumstances and factual information that they presented at the time of the commission of the crime. In other words, they must be able to show that no alteration, deletion, addition or other change has been or cannot be made.
For the above, given the special characteristics, electronic evidence could be defined as information produced, stored, or transmitted in digital form that may later be needed to prove or disprove a disputed fact in a legal process (Miha, 2024).
Based on the non-material nature of data and information stored in electronic form, it can be said that their manipulation is easier compared to traditional forms of evidence. This has created special challenges for the judicial system which requires such data to be handled in a special way, to ensure the inviolability of the evidence that the data provide. Meanwhile, a very important aspect of electronic evidence is its legal provision. Concretely, in the Code of Criminal Procedure, this evidence is not expressly foreseen, but the current provision includes electronic evidence in the field of criminal process evidence. This follows the ratification of the Budapest Convention, an important international criminal justice treaty on cybercrime and electronic evidence.
Specifically related to electronic evidence, in Article 14 of the Convention it is provided that:
" 1. Each Party shall adopt such legislation and other necessary measures to establish the powers and procedures specified in this section due to specific criminal investigations or trials. 2. Except as otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to: a) criminal offenses established in accordance with Articles 2-11 of this Convention; b) other criminal offenses committed through a computer system; and c) collection of facts in electronic form of a criminal offense. ...
And in article 21 of the same Convention, it is provided that: *"1. Each Party will adapt such legislation and other measures, which may be necessary to give power to the competent authorities: a) to collect or register through the application of technical means in the territory of that Party; and b) compel a service provider, within its existing technical capabilities: (i) to collect or record, through the application of technical means in the territory of that Party; or (ii) to cooperate with and assist competent authorities in the collection or recording of traffic data, in real time, accompanied with specified communications in its territory, transmitted through a computer system."* [4]

[4] Council of Europe Convention on Cybercrime (ETS No. 185), accessible at the link: https://www.coe.int/en/web /cybercri me/home .

So, in the correct implementation of the provisions of the Convention, the content of which is also reflected in the Code of Criminal Procedure in 2017, electronic evidence constitutes a new type of evidence that is very important for time and the criminal process.

4. Features of electronic evidence

As it is mentioned above, electronic evidence, in most of its features, is similar to the traditional form of evidence, since basically, just like classical evidence, they constitute evidence in a criminal process and aim to, through their content, to make an irreplaceable contribution to a criminal process. Despite their probative and corroborative purpose, electronic evidence also has some unique characteristics that differentiate it from other classic evidence of a criminal process.

Firstly, electronic evidence enjoys the quality of being invisible to individuals who do not have special knowledge of the use of various technological devices, systems, networks and the internet. This is because electronic evidence is often found in places where only specialists could look for it, or in places accessible only by means of special tools used by them.

Secondly, electronic evidence has a volatile character, since in some devices and under certain conditions, computer memory and the evidence it contains can be corrupted or altered by normal operation or use of the device, without the intent to destroy them. This can be caused, for example, by a power outage or when the system needs to place new information over the old due to memory space. Also, computer memory can become corrupted or lost, due to environmental factors such as excessive heat or humidity, or due to the presence of electromagnetic fields.

Thirdly, electronic evidence has the ability to be copied, multiplied without changing their content. This is because digital information can be copied endlessly and with the same accuracy as the original. This unique feature of electronic evidence, completely impossible for some of the types of classical evidence provided for in the Code of Criminal Procedure, leads us to the argument that multiple copies of evidence can be examined independently and in parallel by different specialists, for various reasons, without affecting the original electronic evidence.

All these characteristics make us better understand their nature, bringing to our attention the increase of continuous knowledge about them, as well as the measures that must be taken to ensure it, with the aim of its valid use in a criminal process. Bearing in mind the above, in fulfilling the purpose of the correct acquisition, handling and use of electronic evidence in a criminal process it is essential that:

- The handling of electronic evidence should be done by specialists in the field, since each type of electronic device has its own specific features, which require the use of special procedures. The non-use of which creates the risk of inadvertent modification of the evidence, which creates problems during the judicial examination, as it relates to the integrity of the data contained in these electronic evidences.
- Specialists in the field must use appropriate procedures, techniques and instru-

ments, as in more traditional forensic disciplines.
- To continuously review and update the procedures and techniques to be used for electronic evidence, as new technologies are developing very quickly and with them electronic evidence and their resources.
- Electronic evidence should always be obtained in accordance with existing legislation and best practices, with the aim of using it in the criminal process.

5. Principles of electronic evidence

Electronic evidence, as one of the newest forms of evidence in a criminal process, needs to be studied and treated with special care and attention. Of course, during this process, the implementation of the legislation should be a priority, but equally important are the principles on which the activity of the various subjects of the criminal process should be based, specifically related to electronic evidence. These principles are provided by the Council of Europe guidelines for electronic evidence and are provided to guide interested parties. Let us see below some of the principles which the prosecuting body and judicial police officers should keep in mind when finding, receiving and securing them.

Firstly, we mention the principle of data integrity, also considered differently as that of the inviolability of evidence. At the core of this principle is the idea that any action taken should not materially change a data, electronic device or means of communication, which can then be used as evidence in court. Electronic devices and data must not be altered.

Secondly, we mention the principle of control traces, through which it must be understood that, for all actions performed for the treatment of electronic data, a document must be created and saved in order to be controlled later. An independent third party must not only be able to repeat these actions, but also achieve the same result. All activity related to the control, seizure, access, storage or transfer of electronic evidence must be fully documented, preserved and available for review whenever required during judicial review.

Thirdly, we mention the principle of specialist support, through which it must be understood that if it can be expected that, during a planned operation, electronic evidence can be found, the person responsible for that operation must necessarily take measures for the presence of specialist's electronic evidence. Of course, such a specialist must have sufficient experience and knowledge as a specialist in this field, but also experience and knowledge in conducting investigations (Pekmezi and Çukaj, 2024).

Another important principle is that of proper training, which is specifically related to the persons securing the scene, who must have the necessary and appropriate training to be able to control and seize electronic evidence when the specialist is not at the scene. Meanwhile, there is also the principle of legality, which for the benefit of electronic evidence has the same power as for any other legal situation of a criminal nature and not only. In any case, people who encounter electronic evidence must

handle it according to the relevant procedures and in a very correct manner. All the above principles must be materialized in practice during the investigative phase, which is headed by the Prosecutor of the case and followed by judicial police officers and specialists in the field of information technology. The importance of implementing these principles applies not only when we are in front of the case of the investigation of criminal offenses in the field of cybernetics, but also during the development of any other criminal process, where electronic evidence helps to clarify the truth and punish its authors. Consequently, it is very important for all those involved in the legal system to become familiar with the different forms of electronic evidence and know how to handle them.

In this perspective, it should always be kept in mind that:

- The Internet has provided opportunities, new strategies for committing crimes. Through new communication channels, new categories and figures of crime have been created.
- Every day, more and more crimes involve an electronic device that has a memory or some kind of programming. Even when the crime itself did not use such a device, the actions of the perpetrator may very well have been fixed or recorded on a camera or through another technological device, which could be a phone, vehicle, etc.
- Evidence can also be found on websites, social networks, e-mails, but also in chat rooms.

6. Sources of electronic evidence

Along with the increase of electronic evidence, its resources are also being increased. The list of their potential sources is not exhaustive. This is implied by the definition that the Budapest Convention itself makes of computer system and computer data. Specifically, "*For the purposes of this Convention: "computer system" means any device or group of devices interconnected or connected to each other, one or more of which, on the basis of a program, performs automatic data processing; "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a suitable program that causes a computer system to perform a function;*"[5]

As noted, this definition is quite broad and covers tablets, smart phones, but also many other devices, not specifically specified. This definition is in line with all cybercrime legislation, which in any case does not set boundaries. This is due to the ever-evolving nature of this crime, as well as the guarantee of a flexible and appropriate legislation with every change in the computer world.

7. Digital and classic forensics

"Digital forensics is a branch of forensic science that focuses on the identification, retrieval, processing, analysis and reporting of electronically stored data. Electronic evidence is a com-

[5] Article 1, Budapest Convention.

ponent of nearly all criminal activity, and digital forensics support is essential to law enforcement investigations. Electronic evidence can be collected from a wide range of sources, such as computers, smartphones, remote storage, unmanned aerial systems, shipboard equipment and more. The primary purpose of digital forensics is to extract data from electronic evidence, process it into actionable intelligence, and present findings for criminal prosecution. All processes use sound forensic techniques to ensure findings are admissible in court."[6]

As noted, Digital Forensic Medicine is a new science, compared to other forensic sciences, which already have a consolidated practice in legal and practical terms. But despite this, the number of cases involving digital electronic evidence is growing rapidly, creating a large gap between experience and knowledge about digital forensics on the one hand, and the fact of increasing cases involving digital evidence on the other. Due to this report, the subjects of the criminal proceedings and especially the prosecution body and judicial police officers should hurry to familiarize themselves with this new science.

Keeping in mind the legal provision of the Budapest Convention, the great variety of technological devices and networks in which computer data constituting electronic evidence can be found, as well as the characteristics of each of them, digital forensics branches into several subcategories. Mention here, Forensic Post Mortem, which is related to how to acquire, process, analyse and report data stored in computer systems which are not powered on. This subcategory is the most traditional of forensic medicine. Live Forensics, which relates to how data stored in live computer systems can be secured, processed, analysed and reported. Compared to Medical Law Post-Mortem is a fairly new subcategory, but it is becoming increasingly important as much data today is stored temporarily, remotely or encrypted. Application Forensics, which is the subcategory that focuses on analysing traces and artifacts left in thousands of different applications. Forensics of other hardware devices, such as digital video recorders, routers, game consoles, sharing devices and much more. Many of these devices have their own file systems and operating systems. Mobile Forensics, which is a fairly new category, but which is becoming quite popular, since many data that may be interesting for an investigation can be stored on mobile devices such as smartphones and tablets. As well as Network Forensics, which deals with electronic evidence that is transmitted over a network, whether wireless or wired, whether the Internet or even a local area network.

Given this vast array of subcategories, finding specialists who can deal with finding and handling electronic evidence remains a challenge. Also, the creation of suitable laboratories for the handling of electronic evidence should be a priority for the Albanian state, despite the cooperation with special international structures such as Eurojust and Europol.

[6] Interpol, accessed at the link: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch,crucial%20for%20laë %20enforcement %20investiga tions .

8. EU's commitment to electronic evidence

"*More than half of all criminal investigations today involve a cross-border request to access electronic evidence such as texts, emails or messaging apps. That's why the Commission is proposing new rules that will make it easier and faster for police and judicial authorities to access the electronic evidence they need in investigations to catch and convict offenders*." This commitment takes on an even greater value in cases of investigation of criminal offenses in the cyber field, for the verification of which electronic evidence is necessary and often the only type of evidence. Based on this need, on 29 November 2022, the European Commission, the European Parliament and the Council reached an interim political agreement on legislation to speed up authorities' access to the digital data needed to investigate and prosecute criminal offences, regardless of where they are located these data. This agreement, following the proposal of the Commission, led to the approval of a Regulation on European orders for the production and preservation of electronic evidence in criminal matters and a Directive on the appointment of legal representatives for the purpose of taking evidence in criminal proceedings. This initiative has been concretized with the approval of Regulation (EU) 2023/1543 on European orders for the production and storage of electronic evidence in criminal proceedings and for the implementation of prison sentences and Directive (EU) 2023/1544,[7] on harmonized rules for the assignment of certain institutions and for the appointment of legal representatives in order to receive electronic evidence through appropriate forms for their direct use in criminal proceedings. The way data is managed and stored affects the usability of electronic evidence, as some service providers store this information in fragmented and different ways and may not always be useful for use in a criminal trial. Thus, this fragmentation creates legal uncertainty for those involved in a criminal process. Also, often this difference in treatment depends on whether service providers, administrators, data custodians offer their services at national level, transnational level, or inside or outside the European Union.

Under these conditions, the new provisions of the legislation on the proceedings under review enable judicial authorities in an EU country to directly request[8] access to electronic evidence held by any service provider in the EU, which is established or represented in one of the EU countries. The new legislation consists of two legislative components. Firstly, the Regulation of the European Parliament and of the Council on European orders for the production and preservation of electronic evidence and secondly the Directive of the Parliament and of the Council on harmonized rules for the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. Specifically, at the level of the EU, the European Preservation Order will operate, through which a judicial authority is addressed to the legal

[7] Directive (EU) 2023/1544 of the European Parliament and of the Council, of 12 July 2023, laying down harmonized rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, accessible at link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.191.01.0181.01.ENG .

[8] Directly in the sense of ordering, without the need for approval, although always through local bodies.

representative in the country/s outside the jurisdiction of the issuing member state, with the aim of activating the disposition and storage of cited data, in readiness for a subsequent request to produce[9] the same previously stored evidence. As well as the European Production Order, which allows judicial authorities in a Member State to obtain electronic evidence (such as email, text or app messages, as well as information to identify a perpetrator as a first step) directly from a service provider or its legal representative in another member state, who will be obliged to respond within 10 days and within 6 hours in emergency cases.

Of course, these mechanisms serve the fight against crime and cybercrime in particular. However, Albania, as a non-member country of the European Union, does not benefit from these provisions, therefore the coordination between different countries, in order to secure the electronic evidence necessary for a criminal process, will continue with the current mechanisms in force, mainly between institutions such as Europol, Eurojust, etc.

9. Conclusions and recommendations

Evidence is one of the most important components of a criminal process, as it leads us to the truth. In today's reality, properties are divided into two categories, in that of classical evidence, which over the years have been consolidated in every aspect, both in legal provisions and in practice, and in electronic evidence, which because they are new, need a special treatment in many aspects. Albania's criminal procedure has made an open legal provision in the context of what can be electronic evidence, thus responding to the obligations of the Albanian state provided for in the Budapest Convention, from the moment of its ratification and at the same time responding to the current development of cybercrime in particular, but also all other types of crimes, the realization of which can be carried out or assisted through technological devices and various information networks.

Thus, evaluating the legal forecast on electronic evidence as a stable forecast in time, as it does not limit, but allows the taking of any new type of evidence, which comes as a result of the day-to-day development of technology, in order to increase efficiency of criminal legislation in the investigation and detection of criminal offenses in the field of cybernetics and all other criminal offenses which are assisted by technological devices, computer systems and various internet networks, as well as to avoid subjectivism in what is an electronic evidence , it is recommended to add a general, but also a special provision for electronic evidence in the Code of Criminal Procedure. This new provision should not be aimed at changing the current one, but at supplementing the current legislation, bringing more clarity to all institutions and professionals whose work involves the handling of electronic evidence.

Meanwhile, despite the good and efficient cooperation with the EUROJUST and EU-

[9] Production, in the sense of being formally administered as evidence, by a local authority, usable in a criminal proceeding, albeit by a court of the country that issued the warrant, and not by the country that administered the evidence in question.

ROPOL structure, under the perspective of Albania's membership in the EU, in order to prepare the ground for the alignment of Albanian legislation with that of the EU, it is important for the Directive 2023/1544 to be recognized and assimilated by the Albanian state. Furthermore, the handling of electronic evidence by specialists in the field, with the aim of using it in a criminal process, remains a challenge. For this, the Albanian state should show an increased interest in the creation of policies to attract these specialists, as well as the creation of suitable laboratories for handling electronic evidence, despite the good possibility of cooperation with special international structures such as Eurojust and Europol.

Finally, the School of Magistrates, which is responsible for the continuing training of magistrates, must take all necessary measures for the training of magistrates on the electronic test. More training helps to create a principled approach applicable in practice to the investigation of criminal offenses based on electronic evidence.

References

Council of Europe Convention on Cybercrime (ETS No. 185), accessible at the link: https://www.coe.int/en/web/cybercrime/home .

Code of Criminal Procedure of the Republic of Albania, amended.

Directive (EU) 2023/1544 of the European Parliament and of the Council, of 12 July 2023, laying down harmonized rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, accessible at link: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3 AOJ.L_.2023.191.01.01 81.01.ENG .

Evaluation report on the taking and use of electronic evidence in criminal proceedings under national legislation in South Eastern Europe and Turkey, accessible at the link: https://rm.coe.int/3156-52-electronic-evidence-report-v4- alb/16808cfd36 .

Interpol, official website, link: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch,crucial%20for% 20law%20enforcement%20investigations .

Miha, E. (2024). Preliminary investigation and invalidity of investigative actions. *European Journal of Economics, Law and Social Sciences, Vol. 8. No. 2.*
DOI: https://doi.org/10.2478/ejels-2024-0009

Miha, E. (2024). Legal changes of the decision not to initiate a proceeding in the Albanian criminal procedure code, their implementation in practice. *Balkan Journal of Interdisciplinary Research, Vol. 10. No. 1.*
DOI: https://doi.org/10.2478/bjir-2024-0008

Pekmezi, I. Çukaj, L. (2024). Criminal offenses in the field of Cybernetics related to computer - Computer forgery and computer fraud. *European Journal of Economics, Law and Social Sciences, Vol. 8. No. 2.*
DOI: https://doi.org/10.2478/ejels-2024-0010