OPEN ACCESS

ISSN: 2835-6764

Cukaj L and Bezati I (2025) 1848
American J Sci Edu Re, 2025; 4(11):100280
DOI: 10.71010/AJSER-2025-e280

Research Article

American Journal of Science Education Research

Investigating Cybercrimes: Combining Law, Technology, And Security

Prof. Asoc. Dr. Lirime Cukaj[1*], Ms. Iliba Bezati[2]

[1]*University of Tirana, Faculty of Law,*
[2]*President of the Court of Appeal of General Jurisdiction of the Republic of Albania. E-mail: ilibabzt@gmail.com; Telf-0696377577*

Abstract
Cybercrimes include illegal acts committed through computer systems and electronic networks, falling into two categories: in the narrow sense, where the security of computer systems and data is hit, and in the broad sense, which include activities such as unauthorized information sharing, support for extremist groups, pornography and pedophilia, fraud and other forms of abuse. With the development of information technology, these crimes have taken on transnational proportions, using advanced programs to hide traces and making it difficult to identify the perpetrators. This makes their investigation very complex, requiring technical expertise, the use of computer forensics tools, international coordination and personal data protection.
The investigation of computer crimes differs from the traditional one due to the digital nature of evidence, its possibilities of manipulation and international distribution. International cooperation is essential for the success of prosecution, but changes in legal frameworks and different capacities of states create additional challenges. In addition to the technical and legal aspect, investigators must ensure respect for the privacy of individuals, protecting personal data during investigative actions. The study of cybercrimes is important not only from a legal perspective, but also from a sociological and criminological perspective, analyzing the way criminal networks interact in a global and interconnected environment, and emphasizing the need for specialized and multidimensional approaches to their prevention, investigation, and punishment.

Keywords*: investigation, cybercrime, cyber system, transnational crimes, international cooperation, letters.*

1. Introduction

In the contemporary era of digital development, cybercrimes are one of the biggest challenges for legal systems and security institutions. A fundamental problem encountered in dealing with them is the lack of a universal and comprehensive definition of these works. Due to the rapid pace of technological development, new forms, methods, and tactics for committing crimes in the virtual space are constantly emerging. However, the common element that unites all these manifestations is the use of computer systems and communication networks as a means of carrying out illegal activities.

Cybercrime can be divided into two main categories[1]:

a) *In the strict sense, computer crime is considered any illegal action or behavior committed through electronic means, which aims to violate the security of computer systems, networks or data processed by them.*

b) *In a broad sense, computer crime includes any illegal action that is carried out by means of a computer or computer system. This includes actions such as unauthorized processing, provision or distribution of information on the network, for the purpose of abusing or encouraging harmful activities, such as supporting terrorist groups, extremists or the dissemination of pornographic and pedophilic materials.*

[*]**Corresponding author:**
Prof. As. Dr. Lirime ÇUKAJ. Email: lilicukaj@yahoo.it

Citation: Cukaj L and Bezati I (2025) Investigating Cybercrimes: Combining Law, Technology, And Security. American J Sci Edu Re: AJSER-280.

Received Date: 05 November, 2025; **Accepted Date:** 13 November, 2025; **Published Date:** 19 November, 2025

Various forms of fraud that compromise the integrity of computer networks, pyramid schemes, credit card fraud, and other similar illegal activities also fall into this category.

The development of information and communication technology has brought tremendous benefits to modern society, transforming the way people communicate, work, and interact. However, in addition to the advancements, this digital age has also brought new challenges in the field of security and legal order. One of the most complex challenges is the rise of cybercrime — a form of criminality that operates in virtual space, where physical boundaries are blurred and perpetrators often remain invisible. Due to their technical nature, these crimes require a specialized approach to investigating and **securing digital evidence**.

Computer crimes have a pronounced **transnational character**, as they are often practiced in more than one state, involving actors and systems operating beyond national jurisdictions. This trait makes them the object of study not only from a legal point of view, but also from a criminological and sociological one, as they represent a social phenomenon related to the way criminal networks interact in an interdependent global environment.

Another important aspect relates to the use of advanced technologies for hiding traces. Perpetrators of cybercrimes often use **encrypted programs** to protect their communications, making it harder for law enforcement authorities to identify them[2]. This phenomenon has also been highlighted by Europol, which has noted the increase in criminal groups employing

[1] MSc. Luljeta Ismajlukaj, *General Directorate of the State Police*, 'Online pornography with children: causes, investigation and prevention' (2018) at the III International Scientific Conference *Computer Crime, Cyber Threat and National Security*, Security Academy, pg. 29.

[2] Some of these popular programs and services include: **Signal, WhatsApp, Telegram (Secret Chats), ProtonMail, PGP/GPG for encrypted emails, Tor, and VPN for anonymizing online traffic, as well as dedicated platforms such as SKY ECC, EncroChat, and ANOM**, which have been used by criminal actors for international activities.
For example, **SKY ECC** has provided an encrypted messaging service that has recently been discovered and used by law enforcement authorities to investigate international criminal organizations.

professional hackers for criminal purposes, a trend that is expected to expand significantly in the coming years[3].

The investigation of crimes in the field of cybernetics differs significantly from the investigation of traditional criminal offenses, as the evidence is not of a material nature, but of an electronic nature; it is easily manipulated, hidden or disappeared. This makes the investigative process more complicated and requires the use of modern computer *forensics* tools, cooperation with IT specialists and coordination with foreign authorities, given that cybercrimes often have an international character. For an individual to commit a crime in the cyber field, only his computer skills, a computer system and the connection to a national or international computer communication networks would be enough.

In the field of cybercrimes, the possibilities of hiding the connection between the criminal offense and its perpetrator, in the virtual field, are very wide. Also, the anonymity offered by the connections on the network, enable the author to be moved from his real location. What also affects the investigation of these criminal offenses is the state infrastructure, which is adapting with slow steps, and taking into account the recent cyber-attacks, [4] we see that in fact the law enforcement bodies have not had the right reaction to fight them, causing us to have low results in the fight against computer crime. Of course, the international nature of cybercrime brings the need for international cooperation between states, but it should also be taken into account the fact that each state has its own nature of investigative activity and under these conditions the levels of cooperation of states vary depending on the state in which the criminal offense lies.

The success or failure of investigations of an international character in the field of technology is closely related to the timely realization and full fulfillment of investigative actions by each of the participating states[5]. In addition to this aspect, another important problem in the investigation of computer crimes is related to the fact that the procedural bodies, while fulfilling legal obligations, are often forced to carry out actions on computer equipment, in which, in addition to the traces of the criminal offense, data pertaining to the private life of individuals can also be found. This situation raises before the procedural body the obligation to guarantee the protection of fundamental rights, ensuring full respect for the private life of the person at every stage of the investigative process. In this context, the investigation of cybercrimes requires the coordination of legal knowledge, technological expertise and security mechanisms, to guarantee effective data protection and to punish the perpetrators of these offences[6].

2. Procedural instruments for the provision of evidence in cybercrimes and the difficulties of their implementation in practice[7]

In the historical framework, the Criminal Procedure Code has undergone significant changes in terms of regulating the means of searching for evidence for cybercrimes. In the 2017 amendments, the controlling role of the court was added and some changes have been made regarding some of the seizure provisions, specifically **Article 208/a of the Code of Criminal Procedure** on the seizure of computer data. Another essential change worth mentioning is Article 8/a[8] of the Code of Criminal Procedure, which has defined an autonomy in the taking of evidence.

Procedural instruments or other means of searching for evidence of cybercrimes include:

1. *Obligation to submit cyber data,*
2. *Seizure of computer data,*
3. *Computer Data Control,*
4. *Interception,*
5. *Computer data storage and discovery.*

- **Obligation to submit cyber data**

We can say that the role of the judiciary has been increased to guarantee and preserve the privacy of the data of other persons related to criminal proceedings, given that human activity is closely related to computer devices and the latter contain data of a personal nature. The court is the competent body which authorizes the investigative activity, orders, upon request of the prosecutor or the injured party, the data holder or controller to submit the computer data stored in a computer system[9].

The collection of user data for computer crime investigations often extends outside the Albanian territory, as most companies that provide major online services (such as *Facebook Inc.*, *Google*, *Microsoft*, *Yahoo*, etc.) are registered abroad and store the information on servers located in other countries. For this reason, the provision of electronic evidence requires

[3] NDTV. (2025, March 18). *Artificial intelligence 'reshaping' organised crime, says Europol.* Retrieved from https://ëëë.ndtv.com/ëorld-neës/artificial-intelligence-reshaping-organised-crime-ëarns-europol-7953697
Ljubas, Z. (2025, March 18). *Europol warns on new tech fueling evolving crime networks.* OCCRP. Retrieved from https://ëëë.occrp.org/en/neës/europol-ëarns-on-neë-tech-fueling-evolving-crime-netëorks

[4] Cyber attacks by the Iranian state in the Republic of Albania.

[5] Armand Gurakuqi (Prosecutor at the Court of First Instance of Tirana), 'Computer Crime Investigation' in *Policing and Security, Cybercrime, Cyber Threat and National Security* (Security Academy, Tirana 2018)

[6] Enisa Shahnini and Ylli Pjeternikaj, *Magistrates*, 'Cross-border access to computer systems and the principle of state sovereignty' (2018) at the III International Scientific *Conference on Computer Crime, Cyber Threat and National Security*, Security Academy, pp. 59–69.

[7] Armand Gurakuqi (Prosecutor at the Court of First Instance of Tirana), 'Computer Crime Investigation' in *Policing and Security, Cybercrime, Cyber Threat and National Security* (Security Academy, Tirana 2018) ibid.

[8] Article 8/a, Evidence, added by law no. 35/2017, dated 30.3.2017 1. Facts in criminal proceedings are proven by any evidence, provided that they do not violate fundamental human rights and freedoms. 2. The procedural body must collect and examine both the evidence that incriminates the defendant and that is in his favor.

[9] Article 191/a of the Code of Criminal Procedure.
Note: This provision also applies to the service provider, so the court can also order the service provider to hand over the information to the subscribers. According to the definition of the Budapest Convention, "Service Provider" means: (i) any public or private entity, which provides its service to users, with the ability to communicate through a computer system; and(ii) any other entity that processes or stores computer data for the benefit of such communication service or users of such service

international cooperation. According to the Criminal Procedure Code, the only instrument for this is **the international letter**, which has a long duration, making it unsuitable for computer crimes that require a quick response and efficient investigative actions. This shows the need for more dynamic and appropriate international cooperation mechanisms for investigations in the field of information technology.

The inefficiency of the application of international letters was considered a significant problem by the Council of Europe during the drafting and adoption of the Budapest Convention. This convention provides for faster and more effective mechanisms for the provision of computer data, including that of users. According to this international act, a signatory state may, ***without directly entering the territory of another state, access or receive data recorded in a computer system of another state, if the requesting party has obtained the lawful and voluntary permission of the person who has legal competence to provide such data.*** This regulation creates the possibility for signatories to use computer communication to address a request for the provision of user data to a company that stores computer data in another country. Obtaining permission from the person legally authorized to hand over the data is crucial and may vary depending on the nature of the data, the specific circumstances, and the applicable legislation. *For example, an e-mail address may be stored by a service provider in another country, or the user himself may store data in another country; in both cases, providing it to law enforcement authorities is only possible when the competent person legally authorizes the voluntary submission of this data.*

Daily practice has identified various problems related to this procedural mechanism. As mentioned above, the receipt of data pursuant to the Budapest Convention, by foreign internet service providers, is based on the **principle of voluntariness.** This principle leaves the provider the discretion to accept or refuse the submission of data. As a result, different international societies follow different policies regarding data submission, creating a non-uniform standard in international cooperation in this field.

- **Seizure of computer data.**

Computer data seizure[10] is a procedural measure that applies only when the data is closely related to the investigation of cybercrimes. According to the Code of Criminal Procedure, this measure is ordered by the court at the request of the prosecutor and determines the right to access, search and receive computer data, as well as the prohibition of further actions on the system. In practice, courts often grant broad authorizations that can include all of the defendant's equipment, exceeding the necessary limits and jeopardizing the individual's privacy. This problem has also been identified in the Albanian case law[11], where decisions allow the seizure and control of various computer systems, including electronic communications, without a clear limitation on data directly related to the object of the investigation.

In addition, the seizure and search can also extend to other computer systems or parts, as long as there are reasonable grounds to think that important data for the investigation is stored there. Implementing these actions includes stopping further actions on the system, obtaining copies of data, and guaranteeing their inviolability, often with the help of specialized experts. The procedure for the seizure of computer systems and data in Albanian legislation does not fully comply with the rules of the Budapest Convention, which limits actions only to information physically stored in the system[12]. The Criminal Procedure Code allows the seizure of data stored outside the territory of Albania, such as email addresses or materials stored by international services, creating problems with the principle of sovereignty and questioning the validity and usability of evidence. For this reason, Albanian provisions should be fulfilled and actions should be limited only to data that are physically located in the territory of the country, in order to ensure compliance with the lawfulness and protection of investigative procedures.

- **Computer data control.**

Law no. 35/2017 added Article 202/a to the Code of Criminal Procedure, which regulates the control of computer data. This article provides that, if there are reasonable grounds to believe that data, information, computer programs or their traces are located in a computer system, including those protected by security measures, the court may make a decision on their control, clearly defining the type of information and the manner of obtaining it, as well as the technical measures that guarantee the preservation of the original data without altering or destroying the content. In investigative practice, the acquisition of data from electronic devices, such as mobile phones, is often carried out through surveillance, but this can jeopardize the integrity of the evidence, as any intervention can change the "hash" value of the data and question its authenticity. For this reason, computer data processing must be carried out by specialized experts, equipped with the necessary technical tools, in order to ensure the administration of evidence without compromising its integrity and maintaining the balance between evidence collection and data protection[13].

- **Interception of communications.**

Another important investigative tool related to computer systems and data is the interception of communications[14], which is allowed for any intentionally committed criminal offense, for which a prison sentence of at least seven years is foreseen. The interception of computer communications is subject to the same legal standards as other private wiretapping, and requires the authorization of the court with a reasoned decision, being done only when it is necessary for the investigation and there is a reasonable doubt that a criminal offense has been committed. In urgent cases, the prosecutor can authorize wiretapping, but within 24 hours a judicial evaluation is required. When communications take place between persons outside Albania, the principle of sovereignty must be respected. **Unlike the case of seizure of computer data, where the Convention provides that the data must be stored within the territory of the party, this requirement does not apply to interception. The reason is related to the fact that the communications that are intercepted take place in real time, are accessible and transmitted through a computer system located in the**

[10] Article 208/a of the Code of Criminal Procedure.

[11] Criminal proceeding no. 8774 of 2014, of the Prosecutor's Office at the Court of First Instance of Tirana.

[12] Article 19, Budapest Convention, "Convention on Cybercrime", ratified by Law No. 8888, dated 25.4.2002.

[13] Armand Gurakuqi (Prosecutor at the Court of First Instance of Tirana), 'Computer Crime Investigation' in *Policing and Security, Cybercrime, Cyber Threat and National Security* (Security Academy, Tirana 2018) page 161.

[14] Article 221 et seq. Code of Criminal Procedure

territory of the state authorizing the interception. Therefore, allowing the interception of computer communications, even in international cases, does not violate the sovereignty of other states.

- **Computer data storage.**

Different countries have **different terms of retention of computer data**, related to users of internet services or communication traffic. From the moment of establishing a criminal fact and making a report by the interested persons, a long period can pass. Also, for the procedures of obtaining these data on the basis of a court decision or by means of a letter of order, a considerable amount of time is necessary. These circumstances can cause the **legal data storage deadlines to be exceeded**, risking their permanent loss. For this reason, **the legislator has provided for the procedure of accelerated storage of computer data**, which is the competence of the prosecutor. The prosecutor may order the expedited storage of certain computer data, including traffic data, when there are sufficient grounds to believe that such data may be lost, damaged, or altered.

According to **Article 299/a of the CPC**, when computer data are in the possession or control of a person, the prosecutor may order their storage and maintenance for up to 90 days, with the possibility of extension only once for reasonable reasons, while the person in charge must keep the proceedings secret until the end of the investigation. Article 299/b provides that the person in charge of storing traffic data shall take all measures to guarantee their validity and to provide the prosecutor's office or the judicial police with sufficient information to identify the service provider and determine the communication route. This mechanism is in line with the Budapest Convention, which allows signatories to request accelerated data storage from other states as well, thus ensuring the inviolability and efficiency of computer evidence, despite long retention periods.

Electronic evidence is also important. Electronic evidence can be defined as information produced, stored, or transmitted in digital form, which can later be used to prove or refute a fact in a legal process. Given the disembodied nature and ease of manipulation of electronic data, this evidence poses particular challenges for the judicial system, which requires special treatment to guarantee its **integrity, authenticity, and inviolability**.

Another problem is related to the legal provision of electronic evidence. There is no clear definition of them in the Code of Criminal Procedure, but in practice they are included in the field of evidence of criminal proceedings, especially after the ratification of the **Budapest Convention**, a key international treaty in the fight against cybercrime and on the recognition and collection of electronic evidence. This situation shows the need for special legal and technical mechanisms, as well as for **fast and secure international cooperation**, to address the challenges of handling, storing and exchanging electronic evidence in criminal investigations.

3. International cooperation in the investigation of cybercrimes.

Elements of computer crime offense figures often span two or more states. For this reason, their investigation is impossible without **international cooperation between the investigative and justice authorities**. The usual procedure for carrying out cooperation in order to obtain evidence outside the Albanian territory is **the letter for abroad**, provided by Article 509 of the Code of Criminal Procedure. Through it, it can be carried out not only the investigative actions necessary for a certain investigative process, but also the receipt of documents, the seizure and control of computer equipment, their expertise and other necessary actions.

The Budapest Convention provides that States Parties shall provide cooperation with each other to the widest extent possible in criminal cases related to computer systems or data, or for the collection of evidence in electronic form for a criminal offence[15]. In urgent cases, signatory states can seek and provide legal aid through secure electronic communication channels[16]. An emergency can be related to the risk of disappearance of computer data, or to criminal offenses that seriously damage a person's property or life.

A very valuable mechanism for the realization of international cooperation is **the 24/7 network of requests and letters (letters rogatory) related to criminal offenses in the cyber field**. The dysfunction of the cooperation between the justice authorities of different countries seriously damages the progress of investigations of criminal offenses in the field of technology, making it impossible to identify the perpetrator of the criminal offense. For this reason, it is necessary to increase the level of cooperation between the investigative and judicial bodies of different countries, to guarantee a quick and efficient investigation.

The Budapest Convention establishes the obligation for States Parties to appoint a contact person to work continuously. The purpose of this network is to provide immediate assistance for the purposes of investigations or trials for criminal offences related to computer systems and data, or for obtaining evidence in electronic form. The assistance provided through the 24/7 network consists of providing technical assistance, expedited data storage, obtaining evidence, providing legal information and locating suspects.

Regarding the implementation of letters, it is found that there are various problems, such as incomplete willingness to offer cooperation, prolongation of execution of requested actions, non-fulfillment of requests for taking evidence due to the high number of letters, partial execution of requests for legal aid or lack of responses. In some cases, letters are not executed at all,

[15] Article 25 of the Convention.

[16] **The Budapest Convention on Cybercrime (2001)** does not specify detailed lists of concrete technologies when talking about "secure means of electronic communication". Its general concept is the use of communication channels that guarantee **the security, confidentiality and integrity of information** during the exchange of requests and data between states parties. Thus, the Convention does not define certain protocols, but states must use electronic means that provide: **data security (encryption), confidentiality of communications, integrity of documents and messages, and control over access by third parties**. In practice, these tools include the use of **encrypted emails (PGP, S/MIME), secure channels for file transfer (SFTP, FTPS), virtual private networks (VPNs**), as well as **dedicated intergovernmental networks for secure information exchange**, internationally recognized as **Europol SIENA** and **INTERPOL I-24/7**.

or there is a lack of accountability, such as from **the Republic of Nigeria** and **the People's Republic of China**[17].

In other criminal proceedings, the return of responses to letters occurs after a long period of time, causing delays in the process, risk of loss of evidence and reduced effectiveness of the investigation. For example, in the framework **of criminal proceedings no. 7345, of 2014, of the Prosecution at the Court of First Instance, Tirana**, for the criminal offense **of "Computer fraud",** the return of the response by the UK justice authorities was carried out about two years after the request for legal aid was sent.

A specific problem is also **the non-execution of letters by the US authorities** in cases of low-risk criminal offenses, such as "Stalking" or "Tampering with computer data". The American authorities prioritize the treatment of high-risk criminal offenses, such as terrorist activity, corruption, crimes against life, leading to the archiving of low-risk cases.

4. Conclusions and problems [18].

4.1. Increase in cybercrimes and challenges for the legal system.

Cybercrimes pose a major challenge for judicial systems and security institutions, due to their digital nature which require specialized technical knowledge [19] , anonymity of their perpetrators and the limitless digital space of committing them. Of course, the lack of a universal definition makes it difficult to build effective legal and investigative mechanisms. Investigating cybercrimes requires a significant time investment, unlike traditional investigations, as processes can take several months or even years. This depends on the complex and often transnational nature of criminal offences, which makes identifying perpetrators and gathering evidence a particular challenge for law enforcement authorities.

4.2. Transnational Character of Cybercrimes

Many computer crimes involve actors and systems operating in more than one country, requiring coordinated and efficient international cooperation to identify perpetrators and gather evidence.

4.3. Use of encrypted technologies and investigative challenges

Perpetrators of cybercrimes use encrypted programs and platforms such as SKY ECC, EncroChat and ANOM, which make it more difficult to collect evidence. This situation requires the use of specialized computer forensics tools, technological expertise and international coordination to guarantee the success of the investigations. Investigating cybercrimes also requires specialized digital forensic equipment and labs, which are lacking in most law enforcement centers. These include the tools and accessories necessary for recording, storing, and analyzing computer data. Finding qualified experts in the field of cybercrimes is also a challenge, as managers of institutions often do not meet the needs for training, staff and equipment, missing out on the opportunity to develop internal capacities.

4.4. The importance of electronic evidence

Electronic evidence, which can be produced, stored or transmitted in digital form, poses particular challenges for the judicial system. Ensuring their integrity, authenticity, and inviolability is essential for their admission to the courts, as well as for punishing offenders**.**

4.5. The role of the legal framework and international cooperation

Legal rules and international instruments, such as the Budapest Convention, and mechanisms such as the 24/7 correspondence network, are indispensable for conducting cyber investigations. International cooperation is imperative for the collection, storage, and exchange of electronic evidence quickly, securely, and legally. Legally, the lack of harmonization of the regulatory framework between states and restrictions on the collection of evidence outside the national territory without international cooperation create huge gaps, making prosecution difficult. Organizational problems are related to the lack of cooperation between national and international authorities, insufficient capacities of the staff of investigators or IT experts, and the high number of cases that exceeds the capacity of institutions.

4.6. Balancing the investigation and the rights of the individual

When conducting investigative actions on computer equipment, the procedural bodies must respect the fundamental rights and private life of individuals, ensuring that the information collected is used only for the purposes of the criminal process and in accordance with the law.

5. Recommendations

To improve the investigation of cybercrimes, it is recommended that:

- investing in specialized training for investigators, prosecutors and technical staff to increase knowledge on information technologies, encryption and analysis of digital evidence.
- Establishment and equipping of digital forensic laboratories for the collection, storage and analysis of computer evidence without compromising their integrity.
- Strengthening international cooperation, by establishing fast and effective mechanisms for data exchange and conducting investigative actions outside national borders.
- Harmonization of the legal framework, clearly limiting the scope of seizures and data control only to information relevant to the investigation, for the respect of privacy and the principle of proportionality.
- Promoting information sharing and awareness among victims and organizations attacked to increase cooperation and the provision of valuable data.
- Establishing strategic plans and internal protocols within institutions for case management, including prioritizing more serious crimes and efficient use of human and technological resources.

[17] Armand Gurakuqi (Prosecutor at the Court of First Instance of Tirana), 'Computer Crime Investigation' in *Policing and Security, Cybercrime, Cyber Threat and National Security* (Security Academy, Tirana 2018) page 164.

[18] Msc Ingrida Behri Mustafa, *High Tech Crimes and Challenges for Their Investigation* (International Academic Conference, OSCE, FDUT, Sapienza University of Rome, Tirana, 21 June 2022) page 407.

[19] The complexity of computer systems and networks, the use of different protocols, VPNs, the TOR network, data encryption, and servers hosted in other countries make it difficult to identify and collect digital evidence.

- **Clear legal definition for electronic evidence:** Domestic legislation should specify the ways in which electronic evidence is collected, stored and used in criminal proceedings, to guarantee its legality and integrity.

Bibliography

1. Law No. 10 054, dated 29.12.2008, *On some additions and amendments to the Law No. 7905, dated 21.03.1995, 'Code of Criminal Procedure of the Republic of Albania', as amended*.
2. Law No. 7905, dated 21.03.1995, *Code of Criminal Procedure of the Republic of Albania*, as amended.
3. Convention on Cybercrime, ratified by Law No. 888, dated 25.04.2002.
4. Gurakuqi, A. (2018). *Computer Crime Investigation*. In *Policing and Security, Cybercrime, Cyber Threat and National Security*. Security Academy, Tirana.
5. Shahnini, E., & Pjeternikaj, Y. (2018). *Cross-border access to computer systems and the principle of state sovereignty*. Paper presented at the III International Scientific Conference on Computer Crime, Cyber Threat and National Security, Security Academy, Tirana.
6. Criminal proceeding No. 8774 of 2014, Prosecutor's Office at the Court of First Instance of Tirana.
7. Ismajlukaj, L. (2018). *Online pornography with children: causes, investigation and prevention*. Paper presented at the III International Scientific Conference on Computer Crime, Cyber Threat and National Security, Security Academy, Tirana.
8. NDTV. (2025, March 18). Artificial intelligence 'reshaping' organised crime, says Europol. Retrieved from https://www.ndtv.com/world-news/artificial-intelligence-reshaping-organised-crime-says-europol-7953697
9. Ljubas, Z. (2025, March 18). Europol warns on new tech fueling evolving crime networks. *OCCRP*. Retrieved from https://www.occrp.org/en/news/europol-warns-on-new-tech-fueling-evolving-crime-networks