Computer Fraud according to the Criminal Legislation of Kosovo

Mirgen Prençe[1]

Anton Martini[2]

Alberto Orlando[3]

Endri Papajorgji[4]

[1]*PhD, "Albanian University", Tirana, Albania*
[2]*PhD (C.), "Barleti" University, Tirana, Albania*
[3]*Dr., Università del Salento, Lecce, Italy*
[4]*Prof. Dr., "Aleksandër Moisiu" University, Durrës, Albania*

Received: 5 July 2026 | ***Accepted: 29 October 2026*** | ***Published: 20 November 2026***

© 2026 Prençe et al.

DOI: 10.56345/ijrdv13n333

Abstract

Technological development and the rapid expansion of information and communication technologies have significantly influenced modern society, creating both new opportunities and new forms of criminal activity. The increasing use of computers, internet services, and digital networks has enabled offenders to commit crimes in ways that were previously impossible, giving rise to the phenomenon of cybercrime. As a result, states are now confronted with major legal and institutional challenges regarding how society should respond to criminal acts committed through technological means that violate social relations protected by criminal law. The complexity, anonymity, and transnational nature of cybercrime make the prevention, investigation, and prosecution of such offenses particularly difficult for criminal justice authorities. Among the various forms of cybercrime, computer fraud has become one of the most widespread and harmful offenses due to its direct impact on property, financial security, and public trust in digital systems. Through the misuse of computer systems, electronic data, or digital platforms, offenders may unlawfully obtain financial or material benefits while causing significant damage to individuals, businesses, and public institutions. In response to these risks, many countries, including the Republic of Kosovo, have adopted specific legal provisions aimed at combating cybercrime and protecting the integrity of information systems. The focus of this paper is the analysis of the criminal offense of "Computer Fraud" as provided for in the Criminal Code of Kosovo. The paper will examine the legal elements and concepts used by the Kosovo legislator in defining this offense, while also addressing the practical challenges related to its implementation. Furthermore, the study will refer to domestic legislation, as well as the Budapest Convention on Cybercrime and other international legal acts that have emerged as a result of this convention, in order to evaluate the extent to which Kosovo's legal framework is aligned with international standards in the fight against cybercrime.

Keywords: ***Technology, computer fraud, computer system, computer data***

1. Introduction

Only a few decades ago, computers were large and bulky devices used mainly by governments, research institutions, and financial institutions. The ability to commit computer crimes was largely limited to those with access and expertise. Today, technology is ubiquitous and increasingly easier to use, ensuring its availability for both offenders and victims (Clough, 2015).

The speed with which the internet has developed, especially in the period following COVID-19, required approaches that could not be addressed solely through the provision of existing criminal offenses in the legislation of Kosovo, but also required the establishment of other institutions, something which the legislator achieved with the entry into force of Law No. 08/L-173 "On Cybersecurity" in 2023.

The entire world has entered an unstoppable era of technological and internet development (Nisha et al.).

The internet is a relatively new phenomenon that has likely affected every type of human activity. Throughout its history, it has changed the way people spend their free time, how they work and communicate with one another, how they entertain themselves, and most importantly, how people think. The internet has changed almost everything, including the ways of doing business and the practices used for this purpose (Dudley et al.).

Considering that in Kosovo the use of information and communication technology has expanded rapidly since the year 2000, it now plays an important role in all aspects of our lives. According to world internet statistics, internet penetration in Kosovo is 90.4%, with 1,693,942 internet users. This trend of internet expansion and the use of devices connected to information technology is comparable to that of developed EU countries. Most institutions in Kosovo have transferred their daily operations online, including organizations that provide services in critical infrastructure sectors such as energy, water, healthcare, transportation, and communications (Strategjia Kombetare per Sigurine Kibernetike 2023-2027, 2023).

In 2010, with the adoption of Law No. 03/L-166 "On the Prevention and Fight against Cybercrime," Kosovo adopted for the first time legislation concerning cyber criminal offenses, which also provided measures for the prevention of cybercrime.

The purpose of this law is the prevention and fight against cybercrime through concrete measures for the prevention, detection, and punishment of perpetrators using computer systems, while guaranteeing respect for human rights. The Convention on Cybercrime served as the basis for the drafting of this law (Abdyli, 2018).

Although Article 15 of Law No. 03/L-166 "On the Prevention and Fight against Cybercrime" is titled "Causing Loss of Property," stipulates that "Causing loss of property to another person by inputting information, altering or deleting computer data, by restricting access to such data, or through any interference with the functioning of a computer system, with the intent of securing an economic benefit for oneself or for another person, shall be punished by imprisonment from three (3) to ten (10) years. For an attempt to commit the criminal offense under paragraph 1 of this Article, the perpetrator shall be punished by imprisonment from three (3) months to one (1) year." It contains elements of the criminal offense of computer fraud, but without expressly including the word "fraud" in its provision, thus making it incomplete.

With the entry into force of Law No. 08/L-173 "On Cybersecurity," published in the Official Gazette of the Republic of Kosovo No. 4 on February 27, 2023, several articles of Law No. 03/L-166 "On the Prevention and Fight against Cybercrime" were repealed.

The criminal offense of computer fraud is provided for in Article 277/K of the Criminal Code of the Republic of Kosovo, introduced by Law No. 08/L-188 on Amending and Supplementing Criminal Code No. 06/L-074. The amending law was published in the Official Gazette of the Republic of Kosovo No. 23 on 23 November 2023. Article 277/K is located in Chapter XXIV/A, entitled "Cybercrimes."

Computer fraud is defined in Article 277/K of the Criminal Code with the following content:

> *"Whoever inputs, alters, deletes, or suppresses computer data, or interferes with the functioning of a computer system, with the intent of securing for himself/herself or another person, through fraud, an unlawful economic benefit or of causing another person a loss of property, shall be punished by imprisonment from one (1) to five (5) years.*
> *When this offense is committed as a member of a group, the perpetrator shall be punished by imprisonment of not less than five (5) years.*
> *For an attempt to commit the criminal offense under paragraph 1 of this Article, the perpetrator shall be punished by imprisonment from three (3) months to one (1) year."*

The structure of Article 277/K closely reflects the model of computer-related fraud contained in Article 8 of the Council of Europe Convention on Cybercrime (Budapest Convention, ETS No. 185). The Convention requires the

criminalization of intentional and unauthorized input, alteration, deletion or suppression of computer data, or interference with the functioning of a computer system, where this causes loss of property and is carried out with fraudulent or dishonest intent to procure an economic benefit. The Convention therefore provides an important comparative and interpretative benchmark for assessing Kosovo's substantive criminal-law framework. References to the Budapest Convention in this paper concern legislative alignment and interpretative guidance rather than an assertion that Kosovo is a Contracting Party to the Convention. In legal doctrine, computer-related offenses are commonly treated as requiring specific legal responses because their object, means of commission, evidentiary traces, and transnational dimension differ in important respects from conventional offenses (Sieber, 1998).

In Article 113 of the Criminal Code, we do not find any definition related to the notions used in the provisions of computer-related criminal offenses.

Computer fraud under Article 277/K shares with ordinary fraud under Article 234 the patrimonial orientation of the offense and the requirement of an unlawful economic benefit or property loss. The decisive difference lies in the mechanism through which the result is produced. Ordinary fraud is based on deception of a person and the resulting disposition of property, whereas computer fraud is committed through manipulation of computer data or interference with the functioning of a computer system. Accordingly, the computer system is not literally "deceived"; rather, it is the technical medium through which the perpetrator produces the unlawful patrimonial result.

This distinction is also important in relation to neighboring cybercrime offenses. Unauthorized access primarily protects the confidentiality and security of a computer system; data interference concerns the integrity or availability of computer data; system interference concerns the functioning or availability of a computer system; and computer-related forgery concerns the authenticity or evidentiary reliability of computer data. By contrast, computer fraud under Article 277/K requires a patrimonial dimension: manipulation of data or interference with a system must be connected to the intent to obtain an unlawful economic benefit or to cause property loss. The same factual episode may involve more than one cybercrime provision, but the legal classification depends on the protected interest, the specific conduct, the required intent, and the result prescribed by each offense. This distinction prevents the broader category of cybercrime from being treated as synonymous with computer fraud.

2. Analysis of the Criminal Offense of Computer Fraud

The criminal offense of computer fraud presupposes the existence of computer data or a computer system, without which the offense cannot be committed in any of the forms provided for by the criminal provision (Raducanu, 2017). Consequently, the interpretation of the offense requires a detailed analysis of the concepts that constitute its essential elements. In the legal framework of Kosovo, these concepts are further clarified through Law No. 08/L-173 on Cybersecurity (2023), which complements the provisions of the Criminal Code of Kosovo relating to cybercrime and the protection of information systems. Considering that the Republic of Kosovo aspires to membership in the European Union, it is required to harmonize its domestic legislation with the acquis communautaire of the European Union. This harmonization is reflected in Law No. 08/L-173 on Cybersecurity, which transposes Directive (EU) 2013/40 of the European Parliament and of the Council on attacks against information systems, as well as Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Through this legislation, Kosovo aims to establish a comprehensive legal framework for the prevention, investigation, and prosecution of cybercrime offenses, including computer fraud.

According to Article 3, paragraph 1.8 of Law No. 08/L-173 on Cybersecurity, computer data refers to any representation of facts, information, or concepts in a form suitable for processing within an information system, including programs capable of enabling the execution of specific functions. Such data may include written documents, photographs, audiovisual materials, software applications, and any other material stored in digital form. The same law defines a computer system as a device or a group of interconnected devices that automatically process computer data through the execution of programmed commands. Furthermore, an information system includes not only the devices themselves but also the data stored, processed, retrieved, or transmitted for purposes related to the functioning, use, protection, or maintenance of those devices. The notion of "interference with the functioning of a computer system" is not expressly defined in Law No. 08/L-173; however, guidance is provided by the explanatory report of the Budapest Convention on Cybercrime. According to the Convention, interference aims to criminalize the intentional obstruction of the lawful use of computer or telecommunications systems through the manipulation or misuse of computer data. The legally protected interest in this context is the ability of operators and users to ensure the uninterrupted and proper functioning of their systems. The Convention intentionally adopts technologically neutral language so that the provision remains

applicable to both existing and future technologies. One of the essential forms of conduct in computer fraud involves the unauthorized inputting of data. This refers to the insertion of correct or incorrect data into a computer system in a manner comparable to the creation of a false document, resulting in unlawful economic gain or damage to another person's property. Another important form is alteration, which may consist of complete or partial modifications to computer data or systems. Brunetta (2017) explains that alteration occurs when a computer system is modified in a way that causes it to function differently from the purpose intended by the lawful holder of the system. Such alterations may occur at any stage of data processing, either directly or indirectly through the manipulation of data intended for future processing (Vicenti, 2015).

Article 277/K of the Criminal Code of Kosovo covers the input, alteration, deletion or suppression of computer data, as well as interference with the functioning of a computer system. These forms of conduct should be interpreted in a technologically neutral manner. In practice, the perpetrator need not perform every manipulation manually: unlawful conduct may be executed through malware, automated scripts, compromised devices, or botnets. Article 8 of the Budapest Convention is likewise formulated in technologically neutral terms, allowing the substantive offense to remain applicable as methods of computer manipulation evolve. T-CY guidance on botnets is relevant in explaining how existing Convention offenses may apply when malicious networks are used as the instrument of the conduct (Cybercrime Convention Committee, 2019). This interpretative approach is also appropriate when examining Article 277/K, provided that all statutory elements of the Kosovo offense are established in the concrete case.

Deletion and suppression of computer data constitute additional forms of conduct relevant to Article 277/K. Legal doctrine may distinguish between the removal of data from an accessible location and conduct that renders data unavailable or inaccessible (Pjeternikaj & Xholi, 2022). For criminal liability, however, terminology should remain tied to the wording of the applicable statutory provision. The conduct must also satisfy the subjective and patrimonial elements required by Article 277/K; a mere interference with data, without the elements required for computer fraud, may instead fall to be assessed under another applicable cybercrime provision.

3. Forms in which the Criminal Offense of Computer Fraud Appears

In recent years, cybercrime has become one of the fastest-growing forms of criminality worldwide, affecting individuals, businesses, financial institutions, and public authorities. Following the COVID-19 pandemic, the increased reliance on digital communication, online services, electronic commerce, and remote work created new opportunities for cybercriminals to exploit vulnerabilities in information systems and online transactions. In this context, the Kosovo Police has repeatedly warned citizens to exercise greater caution when using the internet, emphasizing that both the number and sophistication of cybercriminal offenses have significantly increased after the pandemic period. The rapid digitalization of everyday activities has therefore contributed not only to technological progress, but also to the expansion of criminal activities committed through computer systems and networks. Fraudulent conduct carried out in digital environments takes different forms, ranging from relatively simple fraudulent schemes carried out through electronic mail to highly sophisticated attacks targeting large corporations and financial institutions. According to Putz (2019), some fraud schemes involve basic deception techniques through emails that enable perpetrators to unlawfully obtain substantial amounts of money, while more advanced methods involve carefully organized operations directed against businesses and institutional infrastructures. Due to the continuous advancement of technology, cybercriminals increasingly employ complex software tools and malicious programs to conceal their identities and avoid detection by law enforcement authorities. Computer-related fraudulent schemes may occur in both the private and public sectors, including healthcare systems, insurance companies, banking institutions, tax administrations, and public finance structures (Quang et al.). The broad scope of these offenses demonstrates that cybercrime is not limited to attacks against individuals, but rather represents a serious threat to economic stability, institutional security, and public trust in digital systems. The consequences of computer fraud often include financial losses, identity theft, unauthorized disclosure of confidential information, and disruption of essential services. One common form of computer fraud involves business-related internet fraud. In these cases, perpetrators first gain unauthorized access to a company's computer systems, either through the computer of the business owner or through another device connected to financial transaction data. After monitoring and analyzing the company's financial activities, the offenders intervene during a money transfer transaction by altering banking details and redirecting funds to accounts under their control. The stolen funds are then withdrawn or transferred through multiple accounts in order to conceal the criminal activity (Policia njofton se jane rritur krimet kibernetike, udhezon si te mbroheni, 2020). Such offenses are particularly dangerous because they are often difficult to detect immediately and may result in substantial financial damage to businesses and institutions. From a criminal-law

perspective, however, these practical schemes should not automatically be classified as computer fraud under Article 277/K. The legal classification depends on whether the facts establish the specific statutory acts of data manipulation or system interference, together with the required fraudulent intent and patrimonial purpose or loss. Where the conduct consists mainly of deceiving a human victim—for example, inducing a person to authorize a payment—the facts may instead correspond to ordinary fraud or another offense, potentially in concurrence with cybercrime offenses involving unauthorized access, data, or systems.

Another widespread form of online fraud involves the creation of fake websites that imitate legitimate online shopping platforms or electronic banking services. Through these fraudulent websites, perpetrators deceive internet users into believing that they are accessing authentic and secure digital platforms. Victims are encouraged to provide sensitive personal and banking information, including credit card details, usernames, passwords, and other confidential data. Once this information is obtained, offenders may use it to conduct unauthorized transactions, make online purchases, or sell the stolen data on illegal online markets (Policia njofton se jane rritur krimet kibernetike, udhezon si te mbroheni, 2020). This form of fraud illustrates how cybercriminals exploit the trust of internet users and the increasing dependence on electronic commerce. A particularly common form of online fraud is phishing, which represents a form of digital identity theft. Phishing attacks are generally conducted through electronic mail messages designed to manipulate victims into voluntarily disclosing confidential information, especially online banking credentials and passwords. Typically, the victim receives an email appearing to originate from a legitimate financial institution, informing them of alleged technical problems, security breaches, or urgent verification requirements. The message usually contains a link directing the victim to a fraudulent webpage where they are instructed to enter their personal data. The request is often accompanied by a sense of urgency intended to pressure the victim into acting without verifying the authenticity of the communication. Once the victim provides the requested information, the perpetrators gain control over the victim's banking account and can conduct unauthorized financial transactions (Reccia, 2022). Computer-related fraud is widespread in practice and, due to the manner in which it is committed, it frequently possesses an international character (Miha, 2018). Cybercriminals often operate across multiple jurisdictions, using servers, bank accounts, and digital infrastructures located in different countries. This transnational nature complicates criminal investigations and requires extensive international cooperation among law enforcement agencies, prosecutors, and judicial institutions. Consequently, international legal instruments such as the Budapest Convention on Cybercrime play an essential role in facilitating cooperation and harmonizing legal responses to cybercrime. In practice, computer fraud is frequently committed through devices and systems used for electronic financial transactions and automated services. According to Zlati (2020), such offenses commonly target ATMs (Automated Teller Machines), POS (Point of Sale) terminals, self-service fiscal cash registers, servers of public and financial institutions, and other automated systems used for the payment of goods and services. These may include ticket vending machines for transportation services, coffee and food vending machines, and systems used for utility bill payments. By exploiting vulnerabilities in these systems, perpetrators are able to manipulate transactions, obtain unauthorized financial benefits, or disrupt the normal functioning of services. The increasing dependence on automated technologies therefore requires stronger cybersecurity measures, continuous monitoring of information systems, and the development of effective legal mechanisms aimed at preventing and combating computer fraud. Phishing therefore illustrates the need to distinguish the criminological description of a "cyber fraud" scheme from the narrower legal offense of computer fraud. Phishing may be a preparatory or facilitating technique and does not, by itself, establish every element of Article 277/K. Its final legal characterization depends on what the perpetrator subsequently does with the credentials, data, accounts, or computer systems and on whether the patrimonial elements of the offense are satisfied.

4. Protected Legal Interests

Regarding the protected legal interests in the field of cybercrime, legal doctrine has developed two principal positions concerning the nature of the interests protected by criminal provisions related to computer offenses. The debate primarily focuses on whether cybercrime offenses protect traditional legal interests already recognized in criminal law or whether technological development has created entirely new legal interests that require independent criminal law protection. The first doctrinal position maintains that cybercrime does not create or protect new legal interests, but rather represents only a modern form of committing traditional criminal offenses through technological means. According to this approach, offenses committed through computer systems merely threaten legal interests that have long been protected under criminal law, such as property, privacy, public order, economic security, dignity, and the integrity of communications. In this sense, the use of technology is viewed only as a new instrument or method for committing already existing crimes, including fraud, theft, forgery, defamation, or unauthorized disclosure of confidential information.

This approach has been adopted in several European legal systems, including the criminal legislation of Albania. In

the Albanian Criminal Code, computer-related criminal offenses are not regulated within a separate chapter dedicated exclusively to cybercrime. Instead, these offenses are distributed throughout different sections of the Code depending on the legal interest being protected. For example, offenses affecting property are included among property-related crimes, while offenses affecting privacy or public security are classified accordingly. Through this systematic structure, the Albanian legislator has embraced the doctrinal position that cybercrime constitutes merely a technological manifestation of traditional criminality rather than a completely autonomous category of criminal offenses. The same legislative approach has also been followed by countries such as Italy, Germany, Austria, and Switzerland. These states generally integrate cybercrime provisions within existing criminal law structures, thereby emphasizing the continuity between traditional criminal offenses and offenses committed through computer systems. According to this perspective, the protected legal interests remain fundamentally the same regardless of whether the offense is committed physically or digitally. In contrast, a second doctrinal position argues that the rapid development of information technology and cyberspace has generated entirely new legal interests that require independent protection through criminal legislation. Supporters of this doctrine maintain that computer systems, digital networks, and electronic data have become so essential to modern social, economic, and institutional life that they deserve autonomous legal protection distinct from traditional interests. Consequently, cybercrime is viewed not merely as a variation of conventional criminality, but as a separate category of offenses directed against unique technological interests. This second approach has influenced the legislation of countries such as France and Kosovo, both of which have established separate chapters within their criminal codes specifically dedicated to criminal offenses in the field of cybercrime. By regulating cyber offenses independently, these legal systems recognize that the integrity, confidentiality, availability, and security of computer systems and digital data represent protected interests in their own right. Within this doctrinal framework, legal scholars have introduced concepts such as “computer-related legal interest,” “computer domicile,” and “computer freedom.” The notion of “computer domicile” refers to the protected virtual sphere within computer systems and digital environments, analogous to the protection traditionally afforded to the physical domicile of an individual. Similarly, “computer freedom” relates to the individual’s right to use digital systems, communicate electronically, and maintain control over personal data without unlawful interference. These concepts reflect the growing recognition that technological development has created new dimensions of personal autonomy, privacy, and security that require legal protection. According to Cattaneo (1998), the introduction of specific criminal provisions addressing cybercrime was driven precisely by the necessity of protecting these newly emerging legal interests. As modern societies increasingly depend on digital infrastructures for banking, communication, healthcare, commerce, education, and public administration, attacks against computer systems no longer affect only individual victims but may also endanger broader social and institutional stability. Unauthorized access to information systems, interference with electronic data, attacks against critical infrastructure, and large-scale cyber fraud can produce consequences that extend far beyond traditional forms of criminal harm. Furthermore, the recognition of autonomous legal interests in cyberspace has practical implications for criminal law policy and interpretation. It allows legislators and courts to address cyber offenses more effectively by focusing not only on material damage or economic loss, but also on violations of digital integrity, system functionality, confidentiality, and informational security. This approach also facilitates the adaptation of criminal legislation to future technological developments, ensuring that emerging forms of cyber threats can be addressed even when they do not fit neatly within traditional categories of criminal conduct. The position adopted by the Criminal Code of Kosovo demonstrates a tendency toward recognizing cybercrime as an autonomous field of criminal law protection. By dedicating separate provisions and chapters to cyber offenses, Kosovo’s legislation acknowledges the importance of safeguarding computer systems, electronic data, and digital communications as distinct legal interests. This approach is also consistent with international legal standards established by the Budapest Convention on Cybercrime, which encourages states to adopt comprehensive legal frameworks capable of addressing the unique challenges posed by cybercrime in contemporary society.

5. Conclusion

The analysis shows that Kosovo has developed a more specific substantive criminal-law framework for computer fraud through Article 277/K of the Criminal Code, introduced by Law No. 08/L-188. The structure of the offense is broadly consistent with the model reflected in Article 8 of the Budapest Convention, particularly with regard to manipulation of computer data, interference with computer systems, fraudulent intent, unlawful economic benefit, and property loss. The Convention remains an important comparative and interpretative standard for the analysis of Kosovo legislation.

Law No. 08/L-173 on Cybersecurity, published on 27 February 2023, complements the criminal-law framework by regulating cybersecurity governance, institutional responsibilities, risk management, and the protection of network and

information systems. It also partially repealed the earlier Law No. 03/L-166 on the Prevention and Fight against Cybercrime; the remaining framework of that earlier law was subsequently affected by the 2023 legislative reforms. The relationship between substantive criminal provisions and the cybersecurity framework should therefore be presented carefully: cybersecurity legislation supports prevention, resilience, and institutional coordination, while Article 277/K establishes the elements and sanctions of the criminal offense of computer fraud.

The principal practical challenge is therefore not merely the existence of a criminal provision, but its precise application to rapidly changing forms of digital conduct. Investigators, prosecutors, and courts must distinguish computer fraud from ordinary fraud and from neighboring cybercrime offenses, identify whether the statutory acts concern data or system interference, establish the required fraudulent intent and patrimonial purpose or loss, and preserve electronic evidence capable of linking the conduct to a particular perpetrator. These difficulties become more pronounced when servers, accounts, service providers, victims, or offenders are located in different jurisdictions. International cooperation and technically informed interpretation are consequently central to effective enforcement. Explanatory materials and guidance developed within the Budapest Convention framework can assist in interpreting technologically neutral concepts, but domestic authorities must ultimately apply the precise elements of Kosovo law. Greater consistency in legal terminology, specialized professional capacity, effective preservation and exchange of electronic evidence, and clear differentiation among overlapping cybercrime offenses would strengthen the practical application of Article 277/K and improve legal certainty.

6. Acknowledgment

The authors declare that artificial intelligence (AI) tools were used during the preparation of this manuscript. Specifically, AI-assisted tools were used for language editing, grammatical correction, and improvements in clarity and readability. The intellectual content, analysis, interpretation of results, and final approval of the manuscript remain the sole responsibility of the authors.

References

Abdyli, F. (2018). *Trajtimi i krimit kibernetik sipas legjislacionit të Kosovës dhe roli i policisë në luftën kundër krimit kibernetik*. In *Konferenca e III-të Ndërkombëtare "Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare"*. Tirana, Albania.

Brunetta, N. (2017). *I crimini informatici*. Libreriauniversitaria.it Edizioni.

Cattaneo, A. M. (1998). *Pena e diritto e dignità umana: Saggio sulla filosofia del diritto penale*. Giappichelli.

Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press.

Council of Europe. (2001). Convention on Cybercrime (ETS No. 185), Budapest, 23 November 2001.

Council of Europe. (2001). Explanatory Report to the Convention on Cybercrime (ETS No. 185).

Cybercrime Convention Committee. (2019). *T-CY guidance notes*. Council of Europe. T-CY Guidance Notes

Dewani, D. N., Khan, Z. A., Agarwal, A., Sharma, M., & Khan, S. A. (2022). *Handbook of research on cyber law, data protection, and privacy*. IGI Global.

Dudley, A., Braman, J., & Vincenti, G. (2012). *Investigating cyber law and ethics: Issues, impacts and practices*. Information Science Reference.

Law No. 08/L-173 on Cybersecurity. (2023). Official Gazette of the Republic of Kosovo.

Law No. 08/L-188 on Amending and Supplementing Criminal Code No. 06/L-074 of the Republic of Kosovo. (2023). Official Gazette of the Republic of Kosovo, No. 23, 23 November 2023.

Miha, E. (2018). *Trajtimi i krimit kibernetik sipas legjislacionit të Kosovës dhe roli i policisë në luftën kundër krimit kibernetik*. In *Konferenca e III-të Ndërkombëtare "Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare"*. Tirana, Albania.

Pjeternikaj, Y., & Xholi, A. (2022). *The role of technology in preventing and combating organized crime, financial crimes and corruption*. In *International Academic Conference*. Graphic Line-01.

Putz, J.-L. (2019). *Cybercriminalité: Criminalité informatique en droit luxembourgeois*. Larcier.

Quang, J. J., Bernard, F., & Morgan, M. (2013). *La gestion du risque de fraude*. Emerit Publishing.

Raducanu, R. (2017). Scurte considerații privind sancționarea fraudelor comise prin sisteme informatice și mijloace de plată electronice. *Analele Științifice ale Universității "AL. I. Cuza" Iași, Științe Juridice, 63*(2), 35–45.

Reccia, E. (2022). La tipicità delle più recenti tipologie di frodi informatiche: Necessità di un ripensamento? Un focus sull'attività bancaria. *Archivio Penale, 2*, 1–15.

Sieber, U. (1998). *Legal aspects of computer-related crime in the information society (COMCRIME Study)*. European Commission. COMCRIME Study PDF

Strategjia Kombëtare për Sigurinë Kibernetike 2023–2027. (2023). Government of Kosovo. National Cybersecurity Strategy 2023–2027

Vicenti, E. (2015). *La frode informatica nel quadro della disciplina nazionale e comparata: Prospettive de iure condendo*. Trento.

Zlati, G. (2020). *Tratat de criminalitate informatică* (Vol. 1). Solomon.