International Students Interdisciplinary Scientific Conference Papers

THE HORIZON REVIEW

International Institute for Strategic Research

Journal of International Institute for Strategic Research
International Students Interdisciplinary Scientific Conference Papers

The Horizon Review: Global Perspectives from the International Students Interdisciplinary Scientific Conference

Tbilisi 2023

Editor-in-Chief:
Giorgi Chachkhiani,
Director, International Institute for Strategic Research

For citation use [Author], ["Title of the Paper"], in The Horizon Review: Global Perspectives from the International Students Interdisciplinary Scientific Conference, International Institute for Strategic Research, 2023, [page].

Table of Contents

Giola Cami[60]

Administration of Electronic Evidence in Criminal Proceedings: Regulatory Framework in Albania

Abstract

With the development of Communication and Information Technology, electronic evidence relativity in criminal proceedings has augmented, thus presenting the need to vest the current legislation with proper legal provisions regarding the identification, acquisition, preservation, examination, and analysis of data stored in electronic devices. Understanding the current regulatory framework and criminal proceedings practices are prerequisites for pathing the way to identifying the issues regarding obtaining, seizure, analyzing, and presenting digital evidence. This paper analyzes electronic evidence management legislation under the Budapest Convention and its Annexes, typologies & principles and identifies current challenges in the criminal proceedings related to digital evidence.

This paper addresses challenges by providing an in-depth legal analysis of the Convention, its Annexes, data management provisions in the Criminal Procedural Code of the Republic of Albania, current literature, institutional capacities, and procedural means. It explains how the existing gaps in the legal framework condition effective implementation.

Keywords*: electronic evidence, legislation, challenges, data management*.

Introduction

As technological developments progress and society become more digitized, traditional crimes and cyber offenses involve electronic devices and software tools. Therefore, processing electronic evidence in investigations is an integral part of criminal proceedings. Implications of technology advancements in law have now presented many legal challenges, from legislation approximation to the management of new types of evidence.

The dynamic nature of cybercrimes makes it challenging to implement a coherent legal framework that could harmonize cyber law's legal and technical aspects. The field of digital forensics is still new and challenging, as cybercrime investigations depend on specialized technical expertise to

[60] Giola Cami, PhD Student, University of Szeged (Hungary), Faculty of Law and Political Sciences, Institute of Criminal Law and Criminal Studies, giolacami90@gmail.com.

preserve the authenticity of the evidence. Authorities are provided with legal frameworks that regulate electronic evidence but must be equipped with coherent standardized legal safeguards that can adapt to rapid technological advancements. UNODC has shared the concerns that forensic experts and law enforcement agencies are faced with regarding the question of what it means to ensure accuracy, authenticity, completeness, and convincing evidence.[61] As a result, it is difficult for prosecutor's offices to establish appropriate procedural methods for the identification, seizure, and conservation of evidence during an investigation, jeopardizing the evidence's integrity and affecting its admissibility in Court.

Albania's experience with digital evidence dates back to 2002 when the country ratified the Cybercrime Convention. However, time is required between aligning domestic legislation and establishing effective legal practices to allow law enforcement to tackle novel crimes properly. Guidelines have been incorporated into the National Strategic Action Plan. The central government enhances national initiatives to provide training and equip with proper skills in the judiciary and other legal professions. This study will examine the current Albanian legal framework on electronic evidence, offer a descriptive analysis of criminal provisions regulating it, and seek to map how the legislation was developed under the scope of European legal norms. This paper will be a conceptual framework on *domestic laws*, including the Constitution of the Republic of Albania, Criminal Code, Criminal Procedural Code, relative laws, and guidelines regarding the approximation with the Budapest Convention, *EU framework* under the scope of the Budapest Convention and consequent additional protocols, guidelines, and other legal instruments. Additionally, various concepts and the lifespan of electronic evidence will be examined through descriptive methods concerning the legislation subject to this study, including books, articles, law, or other instruments.

This paper will focus on providing legal analysis to the following inquiries:

- Identify European legal instruments that have framed the current mainframe legislative framework on electronic evidence.
- Analyze Albania's *nunc et situ* regulations governing the use of and access to electronic evidence in criminal proceedings and how they were developed in the scope of Acquis Communautaire.
- Based on judicial experience, assesses potential gaps in the Albanian legal framework on procedural provisions where investigation includes electronic evidence.

The analysis will involve Albanian national legislation as approximated with European *Acquis Communautaire*. The national regulatory framework for obtaining and using electronic evidence will be approached theoretically, within a comparative reference to the legal framework developed

[61] United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, (New York, 2013), 18-27.

by European Opinion under the Budapest Convention. The analysis will aim to understand how the currently developed legal framework addresses the procedural regulation of the identification, seizure, maintenance, and presentation of electronic evidence. The focus of this study will be the integrity of the evidence, considering it a key in criminal proceedings of cybercrimes and others that involve digital evidence.[62] In Albania, the processing of such evidence is approached as per the standards in the Criminal Procedure Code for the admission of any evidence, presenting thus legal and practical problems in terms of the reliability of the electronic evidence and its procurement.[63]. By providing a review of the current regulatory framework regarding digital evidence at the international level and national instruments adapted accordingly, finally, the paper will seek to identify the challenges faced in the current state of electronic evidence legal framework and how they affect the integrity of electronic evidence.

International Instruments

The Council of Europe has significantly impacted the development of the international legal framework - substantive and procedural law- dealing with cybercrime and electronic evidence: the Cybercrime Convention.

The Budapest Convention on Cybercrimes was opened for signature in November 2001, signaling a significant momentum in the legal realm as the most relevant international legal instrument to combat cybercrime and regulate electronic evidence.[64] The Convention established a legal framework to tackle offenses in the cyberspace compound of three elements: (1) Substantive law – identifying and categorizing the novel cybercrimes; (ii) Procedural law – Collections, conservation, and presentation of electronic evidence and (iii) International cooperation.[65] The primary goal of the document is to enable appropriate legislation and the development of a standard criminal policy, with international cooperation regarded as a prerequisite for an effective process. Section two of the Convention is dedicated to developing regulations to provide procedures for managing electronic evidence in criminal proceedings. Thus, we are introducing seven provisions – Articles 15-21 which regulate the following procedural aspects:[66]

Article 15 Conditions and Safeguards – Parties are required to ensure that the establishment, implementation, and application of the Convention's powers and procedures are included in

[62] Vrizlynn L. L. Yinghua Guo, Jill Slay and Jason Beckett, Validation and Verification of Computer Forensic Software Tools-Searching Function, (Digital Forensic Research Conference: Montreal, 2009).
[63] Council of Europe. "Assessment Report on Obtaining and Using Electronic Evidence in Criminal Proceedings under Domestic Legislation in South-Eastern Europe and Turkey." *Https://Rm.Coe.Int/*. Council of Europe, 2018.
[64] Council of Europe, Cybercrime Convention Committee. "Assessment Report on Obtaining and Using Electronic Evidence in Criminal Proceedings under Domestic Legislation in South-Eastern Europe and Turkey." *Https://Rm.Coe.Int/*. Council of Europe, 2018.
[65] Council of Europe. "Budapest Convention on Cybercrime." European Treaty Series-No. 185 (2001).
[66] Council of Europe. "Budapest Convention on Cybercrime." European Treaty Series-No. 185 (2001).

domestic legislation as conditions and safeguards; *Article 16 – Expedited preservation of stored computer data*– Parties are required to adopt domestic legislation that enables authorities to order and obtain the expedited preservation of computer data. *Article 17 – Expedited preservation and partial disclosure of traffic data* - Parties are required to adopt domestic legislation to ensure the obtaining of expedited preservation and disclosure of traffic data; *Article 18 – Production order* - Parties are required to adopt domestic legislation to ensure that authorities are enabled to obtain computer data from natural and legal persona; *Article 19 – Search and seizure of stored computer data* - Parties are required to adopt domestic legislation to ensure that authorities are enabled to seize or access computer data and computer systems; *Article 20 – Real-time collection of traffic data*- Parties are required to enact domestic legislation to ensure that authorities collect and record traffic data in real time using technical means; and *Article 21 –* Interception of content data- Parties are required to enact domestic legislation to ensure that authorities collect and record content data in real time using technical means, for a range for serious offences.

Furthermore, the Council of Europe has developed legal tools to supplement the regulatory framework on digital evidence as above in the scope of its capacity-building programs, such as:

Electronic Evidence Guide. In 2013, the Council of Europe published the most comprehensive guidebook dealing with the analysis of digital evidence[67], updated respectively by Victor Völzow (Germany) under the GLACY Project (Version 2.0) and the CyberEast Project (Version 2.1) of the European Union and Council of Europe. These Guidelines are aimed at supporting partner countries to develop and establish their national protocols regarding digital evidence proceedings, targeting primarily specific roles such as the judiciary, law enforcement, lawyers, and other legal professions. This document provided a legal conceptualization of the processes regarding digital evidence offering a thorough guide and establishing safeguard procedures and standards for the following aspects: Search and Seizure Flow Chart, Live Forensics Flow Chart, Private Sector Preparation Flow Chart, Private Sector Search & Seizure Flow Chart, Acquisition of Digital Evidence Flow Chart and Chain of Custody Record.

Digital Forensics. To contemplate the Electronic Evidence Guide, the Council of Europe published in 2017, "A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory", which provides a guide on the steps in digital forensics after examining the crime scene and collecting primary evidential material. As a result, this document serves as a tool to regulate the activities of digital forensics, beginning with the presentation of electronic evidence for further analysis, including conservation and admissibility in Court.[68]

[67] Council of Europe, Directorate General of Human Rights and Rule of Law. "CoE Electronic Evidence Guide, *A Basic Guide for Police Officers, Prosecutors and Judges*." Https://Www.Coe.Int/En/Web/Cybercrime, (Project on Cybercrime: 2013).

[68] Council of Europe. "Digital Forensics: A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory." GLACY Project Version 1.1 (2017). https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb.

Standard Operating Procedures. In the scope of the CyberSouth Project, in 2019, CoE developed the "Standard Operation Procedures for the collection analysis and presentation of electronic evidence" document offering technical and tactical approached guides intended to be used by judicial and law enforcement authorities. Legal aspects covered here include onsite retrieval, securing, transport, and handling of digital evidence, additionally focusing on analysis and presentation of evidence in courts of law.[69]

In 2021 Council of Europe presented for ratification purposes the Second Additional Protocol to the Convention on Cybercrime, "On Enhanced Cooperation and Disclosure of Electronic Evidence," aiming to develop common international rules to improve cybercrime cooperation and electronic evidence collection for criminal investigations or proceedings. This document proposes safeguards for protecting fundamental rights, focusing on the importance of fostering practical transnational cooperation in criminal investigations, including public and private entities.

National Legislative Instruments

Since the establishment of the democratic regime in 1992, Albania's foreign policy has been pro-western re-dimensioned, with a clear and determined commitment to design a future toward European Union membership. Thus in 2003, we were identified as "Potential Candidate" during the Thessaloniki European Council, and in 2014 we received the "Candidate Country" status. To become a member of the European Union, the applicant country must undertake extensive national reforms, programs, and initiatives that align with the Copenhagen Criteria of Democracy, Rule of Law, and Human Rights. In this regard, a necessity of the process has been to align our current and future national legislative frameworks with the European Union's Acquis Communautaire, including cybercrime legislation. The principles and provisions of the Budapest Convention have served as the foundation for our legal and regulatory framework in developing a national response to cybercrime and crimes committed with the use of electronic devices and digital tools.

On June 20th, Albania ratified the Council of Europe Cybercrime Convention based on Law No.8888/2022, "On the Ratification of Convention for Crime in the Cybernetic Area," stating clearly the commitment to approach the necessity of protecting the community from cybercrimes with priority, by adopting a pertinent legal framework and enhancing international collaboration. Following ratification, both criminal substantive and procedural legislation was amended to include new types of cyber offenses and procedural rules to govern the management of digital evidence.

As a result, substantive law was amended with Law no.10023, dated 27.11.2008, "On some Additions and Amendments to Law no.7895 dated 27.01.1995 Criminal Code of Republic of

[69] Council of Europe. "Standard Operating Procedures for the Collection, Analysis and Presentation of Electronic Evidence," CyberSouth Project, 2019. https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb.

Albania, amended", which added the following new cyber offenses:

- *Article 74/a* Computer-related distribution of pro-genocide or crimes against humanity materials (Article 11 of law no 10 023/2008)
- *Article 84/a* Threat under motives of racism and xenophobia through the computer-based system (Article 12 of law no 10 023/2008)
- *Article 119/a* Distribution of racist or xenophobic materials through the computer-based system (Article 13 of law no 10 023/2008)
- *Article 119/b* Insult under motives of racism and xenophobia through the computer-based system (Article 13 of law no 10 023/2008)
- *Article 143*/b Computer-related fraud (Article 15 of law no 10 023/2008)
- *Article 186/a* Computer falsification (Article 18 of law no 10 023/2008)
- *Article 192/b* Unauthorized computer interference (Article 19 of law no 10 023/2008)
- *Article 293/a*n Unlawful wiring of computer data (Article 23 of law no 10 023/2008)
- *Article 293/b* Interference with computer-related data (Article 23 of law no 10 023/2008)
- *Article 293/c* Interference in computer systems (Article 23 of law no 10 023/2008)
- *Article 293/ç* Misuse of equipment (Article 23 of law no 10 023/2008)

In terms of procedural law legislative amendments, the Criminal Procedural Code (CPC) of Albania was explicitly amended by introducing four new articles that regulate the nature and procedures of electronic evidence following Law No.10054 dated 29.12.2008 "On some amendments to the Criminal Procedural Code amended." The following provisions were added:

- *Article 299/a* Expedited preservation and maintenance of computer data (Article 4 of law no 10054/2008)
- *Article 299/b* Expedited preservation and partial disclosure of computer data Article 4 of law no 10054/2008)
- *Article 191/a* Obligation to produce computer data (Article 2 of law no 10054/2008)
- *Article 208/a* Sequestration of computer data (Article 3 of law no 10054/2008)

Additionally, Law No.9918/2008 "On electronic communication," has provided additional amendments to the procedural law, such as the preservation and administration of data for in criminal proceedings. According to Article 15 (1) of this law, the Authority of Electronic and Postal Communications (AKEP) has the right – following its general authorization right – to include conditions related to: (f) "…*permission for interception by competent authorities defined in the legislation in force on interception of telecommunications and implementation of other liabilities arising out of this legislation*."

As per articles 117-120, law 35/2017 "On several changes and additions to law No.7905 dated 21.03.1995 "Code of Criminal Procedure of Albania" provisioned articles 221-223 of the CPC

regarding communication interception - including provisions on the limits, authorization, and procedure. The table below compares the legal amendments regarding digital evidence in Albania based on the Budapest Convention, including other laws that do not directly deal with the nature of evidence but add to its processing:[70]

Table no.1: Budapest Convention provisions on digital evidence as amended domestically:

Budapest Convention legal provisions	**Criminal Procedural Code** **Albania**	**Amended as per:**
Article 15 – Conditions and safeguards	*Article 221* Limits of permission *Article 222* The decision permitting the interception	Law 35/2017 "On several changes and additions to law No.7905 dated 21.03.1995 "Code of Criminal Procedure of Albania".
Article 16 – Expedited preservation of stored computer data	*Article 299/a* - Expedited preservation and maintenance of the computer data	Law No.10054/2008 "On some amendments to the Criminal Procedural Code amended
	Article 101 "Preservation and administration of data for the purpose of criminal prosecution"	Law no. 9918 /2008 "On electronic communication"
Article 17 – Expedited preservation and partial disclosure of traffic data	*Article 299/b* - Expedited preservation and partial disclosure of computer data	Law No.10054/2008 "On some amendments to the Criminal Procedural Code amended
Article 18 – Production order	*Article 191/a* - Obligation to produce computer data	Law No.10054/2008 "On some amendments to the Criminal Procedural Code amended
Article 19 – Search and seizure of stored computer data	*Article 208/a* - Seizure of computer data	Law No.10054/2008 "On some amendments to the Criminal Procedural Code amended

[70] Council of Europe. "Albania: Cybercrime Legislation, Domestic Equivalent to the Provisions of the Budapest Convention." Octopus Interface Conference, 2020. https://rm.coe.int/octocom-legal-profile-albania/1680a248cd.

Article 20 – Real-time collection of traffic data	Not regulated domestically	
Article 21 – Interception of content data	*Article 221* Limits of permission *Article 222* The decision permitting the interception *Article 223* Actions of interception	Law 35/2017 "On several changes and additions to law No.7905 dated 21.03.1995 "Code of Criminal Procedure of Albania".
Article 25 – General principles relating to mutual assistance	*Article 505* Competencies of the Ministry of Justice *Article 506* Judicial proceedings *Article 507* Execution of rogatory letters *Article 508* Summoning of witnesses requested by a foreign authority	Law No. 10 193/2009 "On jurisdictional relations with foreign authorities in criminal matters"
Article 26 – Spontaneous information	*Article 27* Data transmission without the request of Law No. 10 193/2009 "On jurisdictional relations with foreign authorities in criminal matters"	Law No. 10 193/2009 "On jurisdictional relations with foreign authorities in criminal matters"
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	No domestic regulation	
Article 29 – Expedited preservation of stored computer data	*Article 101* "Preservation and administration of data for the purpose of criminal prosecution"	Law no. 9918 /2008 "On electronic communication"
Article 30 – Expedited disclosure of preserved traffic data	*Article 299/b* - Expedited preservation and partial disclosure of computer data	Law No.10054/2008 "On some amendments to the Criminal Procedural Code amended
Article 31 – Mutual assistance regarding accessing of stored computer data	No domestic regulation	

Article 32 – Trans-border access to stored computer data with consent or where publicly available	No domestic regulation	
Article 33 – Mutual assistance in the real-time collection of traffic data	No domestic regulation	
Article 34 – Mutual Assistance regarding the Interception of content data	No domestic regulation	
Article 35 – 24/7 Network	PoC: Cybercrime Unit, Albania State Police, Ministry of Interior	

Source: Council of Europe, 2020

The final domestic legal instrument is the National Security Strategy Document issued by the Governmental Council of Ministers. Following Decision 1084/2020, the CoM approved the 2020-2025 National Security Strategy on Cybersecurity and Action Plan, which addresses the need for capacity building for investigation teams separately as follows:

Objective 3/C – *Ensure effective investigation to detain criminal offenders in the field of cybercrime*. According to this document, it's of strategic importance to improve the investigation capacities in Albania so that justice can serve the purposes of holding accountable perpetrators through three central policies: (i) providing technical tools to the police and investigative structures; (ii) providing Judiciary, Prosecution Offices, and Police with training -among others, for the purposes of digital evidence usage; (iii) providing training on cybercrimes to be provided in the School of Magistrates and Security Academy; (iv) the development of mechanisms to the State Police to standardize digital evidence analysis and (v) establishing a working group focusing in enabling solutions to issues related to IP users.

Objective 4/A – *Increasing institutional cooperation in the national level.* Three main policy initiatives are provisioned as follows: (i) increasing cooperation and coordination between national institutions in the field of cybersecurity; (ii) providing an instrument to exchange information between institutional focal points, and (iii) forming a national group of experts to assist in the event of a cybersecurity crisis, and assessing the national cybersecurity level.

Objective 4/B – *Increasing international cooperation in cybersecurity matters.* Two main policy initiatives are provisioned as follows: (i) Putting in place effective mechanisms and procedures to facilitate international cooperation and (ii) increasing institutional cooperation and information exchange with NATO/OSCE and other international entities.

Judicial Practice on Electronic Evidence

Decision-making in criminal proceedings has started to address procedural issues related to electronic evidence use and access. Considering that respective amendments in domestic law regarding electronic evidence were made in 2008, the practices provided are few and in progress. Among the judicial jurisprudence, the most prominent decision-making case was that of the Supreme Court following her decision No.147 dated 21.12.2021 regulating the application of provision 208/a of the Criminal Procedural Code of RoA.

Article 208/a Sequestration of computer data:

1. *In cases of proceedings against crimes concerning information technology, the Court, upon request of the prosecutor, shall order the sequestration of computer data or systems. With the same decision, the Court shall establish the right to access, search and take computer data from the computer system and the prohibition to perform further actions or secure the computer data or system.*
2. *Shall there be reasonable grounds to believe that computer data have been stored in another computer system or parts of it, and such data may be legally obtained by, or in the availability of, the initial computer system under control, the Court shall, upon the prosecutor's request, immediately order the search or access to such computer system.*
3. *In executing the court decision, the prosecutor or the judicial police officer authorized by the prosecutor shall adopt measures: a) to prevent any further action being taken or to secure the computer system or part of it or another data storage device; b) to take out and obtain copies of computer data; c) to prevent the access to computer data, or to remove such data from accessible computer systems; ç) to ensure the inviolability of the relevant stored data.*
4. *For the executions of such actions, the prosecutor may order the summoning of an expert who is competent in computer system functioning or the measures applied to protect computer data. The summoned expert may not refuse to conduct his assigned tasks without reasonable grounds.*

The Supreme Court, in this decision-making, has unified the judicial Practice in RoA when dealing with electronic evidence, safeguarding the criteria upon which the Court of Law can allow the sequestration of computer data. The case follows the First Instance Court's decision to allow the Prosecution Office to put computer data under sequestration from the news company Lapsi. al (private) arguing that the evidence in the computer and database of the news company would provide essential evidence for a criminal case investigation. As the case appalled the Supreme Court, it decided to unify the Practice regarding sequestration by investigating the prevalence of rights between public and private interests. Considering that applying sequestration on private property does temporarily limit the right of property possession and consequently of the property right itself, following article 41 of the Constitution of RoA, article 1 of the European Convention

of Human Rights, and article 17 of the Charter of Fundamental Rights of the European Union. Therefore, any limitation in the enjoyment of private property in the scope of the sequestration procedure should be proportional to the need to proceed with it. It cannot violate the freedoms and rights provisioned in the European Convention of Human Rights, signed and ratified by Albania. In light of this legal framework, the Court safeguards the fairness of the balance between citizen rights and the public need to prevent crime. The following three Legal safeguards are provisioned to evaluate the balance and determine the prevalence of the interests:

Necessity. Intervenes or the limitation of any right should be requested only for the needs of public interest and especially be in proportion with the legal purpose it compasses. Such need shall be evaluated by a Court of Law, which will dictate the nature of the case and the importance of the interests as per the provisions of the ECHR judicial case *Pretty v. The United Kingdom, App. No. 2346/02, 29.7.2002, § 70.*

Proportionality. When dealing with computer data, under the principle of proportionality, law enforcement officers should only select necessary systems whose sequestration will limit the least the rights of the owner, as provisioned in ECHR cases Smirnov v. Russia, App. no. 71362/01, 7.6.2007; Draghici v. Portugal, App. No. 43620/10 dated 19.6.2014.

Appropriateness. Under these safeguards, the prosecution office is expected to use the most appropriate legal instruments to serve its interests with the minor legal repercussions for the subjects.

Finally, the Court has referred to the Operational Modules, which dictate that during the sequestration of computer data, only those devices and systems that serve the purpose of the public interest shall be part of the investigation, and no other parts contain data not related to the case.

Can Standardized Legal Safeguards Preserve the Integrity of Digital Evidence?

Following the increased cases involving technology in the 1980s, many legal issues arose that needed to be effectively resolved using the traditional approach. This led to the establishment of computer forensics, vested with the jurisdiction of investigating computer-related crimes. However, as technological advancement preceded and society got more engaged with technology, such conditions paved the way for the advancement of digital forensics, framed as the science of computer investigation and electronic evidence handling that involves the identification, collection, acquisition, and preservation of data found in computers and digital storage[71]. Criminal investigations are heavily reliant on the requirement that data retrieved from computer systems,

[71] Karie, Nickson, and Dr. Simon Maina Karume. "Digital Forensic Readiness in Organizations: Issues and Challenges." Digital Forensics, Security and Law 12 (2017).

networks, and storage devices be collected and analyzed in such a way that evidence integrity and admissibility in Court are preserved.[72]

Because of their non-traditional nature and technical complexities, criminal investigations must be carried out by specialists who have been trained and equipped to deal with electronic evidence, considering the challenges which investigators *face in regard to the preservation of electronics' evidence* integrity in a court of law.[73] This is because, aside from regulations, there are currently no standardized regulations to modulate the authenticity of evidence in digital forensic investigations, resulting in many cases not being able to withstand legal proceedings and due to the nature of the digital data, which is dynamic and volatile and constantly changing.[74]

Such is in the case of Albania, which, as argued in the section above, has now started to build unified judicial practices that establish legal safeguards and principles that would govern unified investigation practices when dealing with electronic evidence. Legal framework and judicial practices in the form of case-law binding practices would make the very foundation of the governance of electronic evidence and condition the integrity of electronic evidence.

Conclusion

Albanian domestic legislation on Electronic Evidence has been developed in accordance with the Budapest Convention on Cybercrimes, its additional protocols, and the Council of Europe's legal instruments in the field. Following our Candidate Status toward the EU Membership, under the requirement of approximation with the European legal framework, Albania has amended its legislation accordingly within the principles of the European Convention of Human Rights, and domestic judicial decision-making should take a referral to practices as established by the jurisprudence of European Court of Human Rights.

Regarding the regulatory framework of electronic evidence, this study examined international developments within the European Union, finding that the Council of Europe's framework has been developed significantly, enabling signatory countries to combat cybercrimes, and is working toward building national capabilities to work with electronic evidence. As well, normative analysis of Albania's *nunc et situ* regulations governing the use of and access to electronic evidence in criminal proceedings are developed strictly under the European framework and found to be constructive and in accordance with Budapest Convention.

---

[72] Sallavaci, Oriola, and George Carlisle. "Procedural Aspects of the New Regime for the Admissibility of Expert Evidence: What the Digital Forensic Expert Needs to Know." International Journal of Electronic Security and Digital Forensics, no. 5 (2013), 161–71.

[73] Karie, Nickson and Venter, H.s. "Towards a framework for enhancing potential digital evidence presentation, Information Security for South Africa", Proceedings *of the ISSA 2013 Conference*, (Johannesburg: 2013), 1-8.

[74] Reedy, Paul. "Interpol Review of Digital Evidence 2016 - 2019" , Forensic Science International: Synergy Vol. 2,(2020): 489–520.

However, considering the dynamic development of Communication and Information Technology, many challenges present the need to establish a firm yet elastic legislation that could address new aspects and issues. Equally important, considering that judicial jurisprudence is yet to develop well-grounded legal practices on different aspects of electronic evidence, there is a lack of standardized safeguards which would rudder the principles of electronic evidence governing criminal proceedings. Such is the case of Albania, wherein in the current judicial jurisprudence, there are few legally binding practices to serve as cooperative principles according to which electronic evidence identification, collection, and management should be guided.

This paper thus addresses the need to establish a set of defined standards and principles regarding the seizure, management, and presentation of electronic evidence, which would preserve the integrity of the electronic evidence in front of a court of law.

Bibliography

1. Council of Europe, Cybercrime Convention Committee. "Assessment Report on Obtaining and Using Electronic Evidence in Criminal Proceedings under Domestic Legislation in South-Eastern Europe and Turkey." *Https://Rm.Coe.Int/*. Council of Europe, 2018.

2. Council of Europe, Directorate General of Human Rights and Rule of Law. "CoE Electronic Evidence Guide, *A Basic Guide for Police Officers, Prosecutors and Judges*." Https://Www.Coe.Int/En/Web/Cybercrime, Project on Cybercrime, 2013.

3. Council of Europe. "Albania: Cybercrime Legislation, Domestic Equivalent to the Provisions of the Budapest Convention." Octopus Interface Conference, 2020. https://rm.coe.int/octocom-legal-profile-albania/1680a248cd.

4. Council of Europe. "Assessment Report on Obtaining and Using Electronic Evidence in Criminal Proceedings under Domestic Legislation in South-Eastern Europe and Turkey." *Https://Rm.Coe.Int/*. Council of Europe, 2018.

5. Council of Europe. "Budapest Convention on Cybercrime." European Treaty Series-No. 185 (2001).

6. Council of Europe. "Digital Forensics: A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory." GLACY Project Version 1.1, 2017. https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb.

7. Council of Europe. "Standard Operating Procedures for the Collection, Analysis and Presentation of Electronic Evidence," CyberSouth Project, 2019. https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb.

8. Criminal Code of the Republic of Albania.

9. Criminal Procedural Code of the Republic of Albania.

10. Karie, Nickson and Venter, H.s. "Towards a framework for enhancing potential digital evidence presentation, Information Security for South Africa", Proceedings *of the ISSA 2013 Conference*, Johannesburg, 2013.

11. Karie, Nickson, and Dr. Simon Maina Karume. "Digital Forensic Readiness in Organizations: Issues and Challenges." Digital Forensics, Security and Law 12, 2017.

12. Reedy, Paul. "Interpol Review of Digital Evidence 2016 - 2019", Forensic Science International: Synergy Vol. 2, 2020.

13. Sallavaci, Oriola, and George Carlisle. "Procedural Aspects of the New Regime for the Admissibility of Expert Evidence: What the Digital Forensic Expert Needs to Know." International Journal of Electronic Security and Digital Forensics, no. 5, 2013.

14. Supreme Court of Albania, Decision No.147 dated 21.12.2021.

15. United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, New York, 2013.

16. Vrizlynn L. L. Yinghua Guo, Jill Slay and Jason Beckett, Validation and Verification of Computer Forensic Software Tools-Searching Function, Digital Forensic Research Conference, Montreal, 2009.