Articles

Studia Iuridica Lublinensia vol. 33, 5, 2024
DOI: 10.17951/sil.2024.33.5.11-30

Giola Cami
University of Szeged, Hungary
ORCID: 0009-0002-1780-9829
cami.giola@stud.u-szeged.hu

Legal Standards for Cross-Border Access to Electronic Evidence in Criminal Procedure: An Albanian Perspective on International Standards*

Standardy prawne dla transgranicznego dostępu do dowodów elektronicznych w postępowaniu karnym. Albańska perspektywa standardów międzynarodowych

ABSTRACT

With the development of Information and Communication Technology and digitalization usage expanding significantly in the society, the production and transmitting of data is evermore based on the means of cloud computing. Consequently, the relevance of electronic evidence in criminal proceedings has augmented, encompassing both cybercrimes and traditional offences. Considering the borderless nature of data exchange, supranational regulations and cooperation, the gathering of e-evidence presents a challenging process for criminal proceedings, particularly when it comes to human rights' implication. Examining the Council of Europe and European Union frameworks on the handling of electronic evidence, the study assesses in particular the procedures and legal issues concerning cross-border electronic data exchange within different jurisdictions in the realm of criminal procedure. The main focus is on the Albanian experience, conducting a comparative analysis on the country's compliance with electronic evidence rules, whilst addressing data protection safeguards in criminal procedure.

Keywords: data transfer; supranational regulations; jurisdictions; criminal procedure

CORRESPONDENCE ADDRESS: Giola Cami, PhD Candidate, University of Szeged, Faculty of Law, Institute of Criminal Law (BTI), H6721 Szeged, Bocskai u. 10-12, Hungary.

* The research was supported by the Digital Society Competence Centre of the Humanities and Social Sciences Cluster of the Centre of Excellence for Interdisciplinary Research, Development and Innovation of the University of Szeged. The author is a member of the "Artificial Intelligence and the Legal Order" research group.

INTRODUCTION

Increased digitalization in the daily interaction, whether personal engagement or business related, has significantly enhanced the relevance of cloud computing in criminal investigations.[1] Hence, considering that exchange of data takes place in a transnational order, the collection of electronic evidence is significantly occurring through the cross-border acquisition procedure. This has presented the law enforcement with notable challenges, including, but not limited to, jurisdictional conflicts, supranational cooperation, singular attributes of the data pertaining volatility, capacity building[2] and/or accessing of the e-data from third-parties. Peculiarly, the collection of data from the service providers constitutes an important procedural aspect in criminal proceedings, as the primary source of electronic evidence often needs to be obtained from private entities.[3] The in-place procedure sustaining international cooperation between law enforcements governed by mutual legal assistance (MLA), provided protracted timeframes which are not conducive to procedural efficiency.[4]

Within the field of criminal procedure, hence, two frameworks have been developed to remedy the procedure of obtaining cross-border access to electronic evidence directly from service providers: (i) Council of Europe framework, comprised of the Budapest Convention and Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, and (ii) EU Regulation 2023/1543.

Whilst both frameworks provide facilitation of obtaining e-evidence through the direct cross-border cooperation between law enforcement authorities and service

---

[1] A. Rosano, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le proposte della Commissione europea sugli ordini di produzione e convervazione di prove elettroniche (e-evidence)*, "La Legislazione Penale" 2020, p. 2; C. Karagiannis, K. Verdigis, *Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal*, "Information" 2021, vol. 12(5), p. 181.

[2] United Nations Office on Drugs and Crime in *Comprehensive Study on Cybercrime* (New York 2013) expressed its concerns about the ability of professionals in forensics and law enforcement to interpret features of electronic evidence such as authenticity, legitimacy and completeness.

[3] European Commission addressed in its official website the proposal for new legal instruments – European Production and Preservation Order (now enforced under Regulation 1543/2023). It provided data according to which in two-thirds investigations involving electronic evidence, there is a need to request evidence service providers based in another jurisdiction. See European Commission, *Frequently Asked Questions: New EU Rules to Obtain Electronic Evidence*, 17.4.2018, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345?gclid=CjwKCAiA_aGuBhACEiwAly57McBWp6fAuIri-3Hwc9lsVHVNHRqij3Bdz5kERTjzM_R-YrNvy19l6BRoCND4QAvD_BwE (access: 12.12.2024).

[4] E. De Busser, *The Digital Unfitness of Mutual Legal Assistance*, "Security and Human Rights" 2018, vol. 28(1–4), p. 163; S. Tosza, *Gathering Electronic Evidence for Administrative Investigations*, "Eucrim" 2023, no. 2, p. 216; European Commission, *Frequently Asked Questions…* The European Commission emphasized that the process of obtaining electronic data extraterritorially through the Mutual Legal Assistance procedure typically takes approx. 10 months.

providers, the legal regulation has been subjected to concerns regarding the data integrity pertaining to human rights' implication.[5]

Within the existing international criminal legislation governed by Council of Europe proceedings on e-evidence collection, rules have been established on requiring firm protection of privacy rights for individuals, while ensuring compliance with the rigorous data protection standards.[6] The Budapest Convention established MLA as the framework for facilitating foreign law enforcement cooperation in evidence collection for criminal proceedings. Twenty years later, the Second Additional Protocol enabled law enforcement direct access to certain types of data from service providers.[7] Within the means of this instrument, the application of Articles 6 and 7 is concerned to potentially create asymmetry with regard to national law of the ratifying country, and potentially implicate data integrity concerns.[8] Under the European Union framework of mutual trust, Regulation 2023/1543 provides standards and guaranties for Member States authorities to access data in extra-territorial jurisdictions.[9] Concerns related to this legal remedy involve the vesting of private entities with public competences and data protection safeguard, within the cross-border context.[10]

The present study assesses (i) rules governing cross-border access of electronic evidence within the criminal procedure in international and European law, (ii) potential implications of data integrity pertaining human rights violation during the cross-border acquisition of electronic evidence, and (iii) a case study of Albania.[11]

---

[5] S. Carrera, G. González Fuster, E. Guild, V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, Brussels 2015.

[6] Convention on Cybercrime, Budapest, 23.11.2001, ETS No. 185, see Article 15 entitled "Conditions and Safeguards"; Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Strasbourg, 12.5.2022, CETS No. 224, hereinafter: the Second Additional Protocol.

[7] Articles 6 to 8 of the Second Additional Protocol. The Protocol indicates international cooperation through direct access of data for subscriber data only.

[8] V. Alimonti, *Assessing New Protocol to the Cybercrime Convention in Latin America: Concerns, Human Rights Considerations, and Mitigation Strategies*, https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam.pdf (access: 10.12.2024).

[9] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ EU L 191/118, 28.7.2023).

[10] V. Mitsilegas, *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence*, "Maastricht Journal of European and Comparative Law" 2018, vol. 25(3), p. 263; S. Tosza, *op. cit.*, p. 216.

[11] Republic of Albania ratified the Budapest Convention on Cybercrime in 2002 and signed the Second Additional Protocol in 2021. Furthermore, having been granted the Candidate status to EU Membership Albania is currently harmonizing its national legislation with EU *acquis*. For the purpose of this study, Albania's criminal procedural law will be assessed from two perspectives. Firstly, employing a comparative analysis, it will assess the compliance of national law with the Council

METHODOLOGY

This study is conducted as doctrinal legal assessment, by providing an in-law analysis of both regulations and literature. The first part of the study is a descriptive analysis and theoretical legal assessment of the state of regulations on international and European law. The second part, using the comparative method, consists of a *de lege lata* analysis of the Albanian legal norms on electronic evidence and data protection. The study focuses on the examination of legal regime on (i) criminal procedural law regulations governing cross-border collection of electronic evidence and (ii) assessment of data protection safeguards in the criminal procedure.

RESEARCH AND DISCUSSION

1. Cross-border access to electronic evidence and data protection safeguards

1.1. Council of Europe package on electronic evidence

The Council of Europe framework is considered to be the most comprehensive international framework governing cybercrimes and establishing international rules for cross-border electronic evidence.[12] The Council of Europe package includes the Budapest Convention and the Second Additional Protocol of binding nature upon the ratification from signatory parties.[13] The framework's regulative norms constituting of (i) criminalization of crimes committed in the cyberspace, (ii) procedural powers to acquire electronic evidence and (iii) international cooperation, are supported by capacity-building programs aiming to strengthen criminal justice capacities.[14] The

of Europe standards and regulations pertaining to electronic evidence in criminal procedures, with a specific focus on cross-border acquisition practices. Secondly, it will discuss on the role of the *acquis communautaire* toward the strengthening of national law and the significance of referring to it in the legal interpretation of procedural aspects related to e-evidence.

[12] Council of Europe, *Joining the Convention on Cybercrime: Benefits*, 8.2.2024, https://rm.coe.int/cyber-buda-benefits-8-february-2024-en-2776-0534-0937-v-1/1680ae70ee (access: 10.12.2024); Council of Europe, *The Budapest Convention on Cybercrime: Benefits and Impact in Practice*, Strasbourg, 13.7.2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (access: 10.12.2024). Data subjected on the study indicates that as of 2020, 177 states were in the process of amending (or had done so) their legislation on the matter, whilst 153 members of the United Nations had used the Budapest Convention as a guideline.

[13] Status as of 14 February, the Budapest Convention has been ratified by 69 parties, whilst the Second Additional Protocol has been ratified by Serbia and Japan only, whilst 41 other signatory countries are yet to proceed with the ratification process.

[14] Within the means of Article 46 of the Budapest Convention, Cybercrime Convention Committee (T-CY) has been mandated with the effective implementation of the Convention, by providing

Budapest Convention, congruently, outlines regulations in substantive law, concerning the criminalization of offences,[15] and addresses criminal procedural powers regulating investigations and the acquisition of electronic evidence.[16] Upon the Budapest Convention and Protocol(s) coming into force, ratifying parties have amended their national criminal laws to ensure that the offences outlined in the Convention are criminalized domestically, along with providing the procedural powers, necessary for criminal justice authorities to conduct investigations. Compatible domestic law aligned with the Council of Europe framework allows for facilitated international cooperation[17] by meeting the criteria of dual criminality.[18] Within the framework of the Council of Europe, more than 60 countries worldwide have adopted comparable laws pertaining to electronic evidence, involving a standardized categorization of the electronic evidence constituted by the subscriber information, traffic data and content data.[19] Furthermore, despite their non-binding nature, the Council of Europe provided two legal instruments namely the Standard Operating Procedures, aiming to serve as technical guide on procedural capacities governing the collection, analysis and presentation of electronic evidence through the chain custody lifecycle,[20] and Electronic Evidence Guide providing legal standards to ensure authenticity of electronic evidence and legal admissibility in a court of law.[21] In particular, the Electronic Evidence Guide has provided legal standards aiming at safeguarding the integrity criteria of the evidence such as authenticity, completeness, reliability, believability

advisory support and information on legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form. For this purpose, capacity building projects have been running alongside since with the participation of ratifying parties, where the main programs include GLACY+, CyberSouth, CyberEast, iPROCEEDS (I+II), Octopus Project, CyberCrime@EAP (I–III) among others. See Council of Europe, *Worldwide Capacity Building*, https://www.coe.int/en/web/cybercrime/capacity-building-programmes (access: 12.12.2024).

[15] Substantive criminal law offences are provisioned accordingly in Articles 2 to 12 of the Budapest Convention.

[16] Council of Europe, *Joining the Convention on Cybercrime*…; Council of Europe, *The Budapest Convention on Cybercrime…* See also Articles 14 to 21 of the Budapest Convention.

[17] Council of Europe, *Joining the Convention on Cybercrime*…; Council of Europe, *The Budapest Convention on Cybercrime…* See Articles 23 to 35 of the Budapest Convention. The Budapest Convention lays out rules for international cooperation between the parties based on the mechanism of Mutual Legal Agreement.

[18] Council of Europe, *The Budapest Convention on Cybercrime…*, p. 5.

[19] Respectively the provisioning of types of e-evidence under the Budapest Convention has been regulated by Article 18 (3) (subscriber data), Article 1 (d) (traffic data), and para. 209 of the *Explanatory Report to the Convention on Cybercrime* (content data).

[20] Cybercrime Programme Office of the Council of Europe, *Standard Operating Procedures for the Collection, Analysis and Presentation of Electronic Evidence*, 12.9.2019, https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb (access: 10.12.2024).

[21] N. Jones, E. George, F.I. Mérida, U. Rasmussen, V. Völzow, *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges*, Strasbourg 2019, https://rm.coe.int/0900001680a22757 (access: 10.12.2024).

and proportionality, which align and contemplate the principles of data integrity, audit trail, capacity building and legality.[22]

This standardized approach fosters enhanced international cooperation in criminal justice efforts concerning electronic evidence. Within the Budapest Convention, the international cooperation between members is based on the mechanism of MLA between justice authorities, whilst the national designated 24/7 Point of Contact (PoC) will allow for a real-time handling of requests and support in immediate assistance.[23] The mutual assistance tool allows access to stored computer data and facilitates the collection of electronic evidence for the purposes of any criminal offence involving electronic data.[24] The assessment study on the applicability of MLA suggests that law enforcement authorities are more prone to obtain information through direct police-to-police collaboration and direct engagement with service providers to obtain subscriber or traffic data, rather than utilizing MLA, attributed to the perceived lengthy procedures and complexities.[25]

Twenty years later, in acknowledgement of the complex legal issues concerning the obtaining of electronic evidence due to the territorial boundaries, constrained capacity of law enforcement to investigate cybercrimes in a timely manner and the need for efficient international cooperation, Council of Europe introduced the Second Additional Protocol in 2021.[26] The Protocol enhances international cooperation and

[22] The document has specifically addressed that while the admissibility of electronic evidence is subject to national law, the standards and principles outlined in the document, which align with the Budapest Convention, are intended to function as a legal reference for criminal justice authorities in domestic criminal proceedings. These guidelines can be adopted while considering the specificities of domestic law.

[23] Council of Europe, *Joining the Convention on Cybercrime*…; Council of Europe, *The Budapest Convention on Cybercrime…* See also Article 35 of the Budapest Convention.

[24] Pursuant to Articles 14 and 23 of the Budapest Convention extends the purpose of the MLA as an instrument for evidence gathering not only within the meaning of the criminal offences under Articles 2 to 12 of this Convention, but also other type of crimes that are committed through the means of the electronic evidence.

[25] In 2014 the Cybercrime Convention Committee delivered the T-CY assessment report on the MLA provisions of the Budapest Convention, where it delivered the result of the study conducted with criminal justice authorities with parties to the Convention indicating the result of a preference by them to avoid the MLA. See Council of Europe, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, https://rm.coe.int/16802e726c (access: 10.12.2024).

[26] Council of Europe addresses the challenges criminal justice is faced with, conveying the need to amend legislation so that it provides direct cooperation with service providers as a remedy tool for more efficient criminal proceedings as per the following documents: (i) Draft Protocol version 2 on the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, issued by CoE prepared by the Cybercrime Convention Committee (T-CY) in April 2021 (https://rm.coe.int/2nd-additional-protocol-budapest-convention-en/1680a2219c) and followed by (ii) the Explanatory Report on November 2021 (https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b).

facilitates the gathering of electronic evidence in a cross-border landscape through the direct access to service providers. The regulation provisions stipulate the issuance of requests on domain name registration and disclosure of subscriber information data directly from service providers.[27] Additionally, it provides the means of emergency mutual assistance to enhance efficiency in cooperation between parties.[28] The relatively new instrument has been subject to legal scrutiny in regards to (i) removing national authorities' role in vetting out the compatibility of the request on the ground of human rights considerations, whilst vesting private entities with judicial power,[29] and (ii) the concerns related to data protection safeguards when personal data is shared with third countries for law enforcement purposes.[30] Within the scope of the data protection safeguards, the Council of Europe framework is enshrined in the European Convention of Human Rights and Fundamental Freedoms (ECHR) and United Nations International Covenant on Civil and Political Rights, whilst ensuring that the implementation of the framework complies with safeguards as provisioned in the domestic law.[31] Additionally, the Council of Europe framework addresses the protection of personal data, as conferred within the means of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

In interpretation to the data protection safeguards within the framework, there is no guarantee that parties to the Budapest Convention and Second Additional Protocol will uniformly benefit from the same level of protection. Article 13 of the

---

[27] Council of Europe, *Joining the Convention on Cybercrime…*; Council of Europe, *The Budapest Convention on Cybercrime…* See also Articles 6 and 7 of the Second Additional Protocol.

[28] Article 10 of the Second Additional Protocol provides for an expedited procedure for mutual assistance requests in situations when there is a significant and imminent risk to the life or safety of any natural person (emergency interpretation under Article 3 (2) (c) of the Second Additional Protocol).

[29] V. Alimonti, *op. cit.*, pp. 10–11; A. Rosanò, *op. cit.*, p. 12.

[30] European Data Protection Board delivers its comments on the Second Additional Protocol through the 2021 document entitled *EDPB Contribution to the 6th Round of Consultations on the Draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime* (Brussels, 4.5.2021, https://rm.coe.int/0900001680a26108, access: 12.12.2024). It notes that several parties to the Budapest Convention are neither members of the Council of Europe nor signatories to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.1.1981, ETS No. 108). Similarly, Council of Bars and Law Societies Europe submitted in 2021 their comments on the Additional Protocol through the document *CCBE Comments on the Draft 2nd Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence* (30.4.2021, https://rm.coe.int/0900001680a25786, access: 10.12.2024) where they re-affirmed their position on setting minimum requirements for ensuring respect of fundamental rights. Furthermore, AccessNow delivered their commentaries on the matter in the 2021 document *Access Now's Comments on the Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime* (30.4.2021, https://rm.coe.int/0900001680a25783, access: 12.12.2024, p. 2), noting as following: "The provisions of the 2nd Additional Protocol on data protection safeguards, data transfer, judicial remedy and oversights are highly problematic and would need to be re-assessed".

[31] Council of Europe, *Joining the Convention on Cybercrime…*; Council of Europe, *The Budapest Convention on Cybercrime…* See also Article 15 of the Budapest Convention.

Second Additional Protocol, in accordance with Article 15 of the Budapest Convention, states clearly that the powers and procedures outlined in the Protocol must be subject to safeguards within domestic law. This raises particular concerns, especially considering that several parties lack a comprehensive data protection framework.

1.2. Mutual trust framework within the European Union

With the Treaty of Lisbon entering into force in 2009, significant transformation of competences within the area of security, freedom and justice took place. Particularly within the realm of criminal justice and police cooperation, Article 82 of the Treaty on the Functioning of the European Union (TFEU) profoundly remodeled the legal landscape within the means of the framework of mutual trust.[32] Hence, cooperation on criminal matters within the EU's jurisdiction would be facilitated through the approximation of the national criminal laws, both substantive and procedural law. Governed by the mutual trust framework, the principle of mutual recognition ensures that a judicial decision issued by authorities in a Member State would equally be enforced in the territory of another member's jurisdiction.[33] This framework served as the backbone for the development of the EU cooperation instruments in criminal matters constituted by Directive 2014/41/EU regarding the European Investigation Order in criminal matters, Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, and European Warrant Arrest framework.[34]

Within the new instruments developed *per se*, judicial and police cooperation within criminal procedure pertaining direct access to third parties within EU jurisdiction is conveyed through the means of the European Investigation Order.[35] It provides the background supporting investigative measures in order to allow

[32] K. Karsai, *Division of Competences between Member States and the European Union in Criminal Procedural Law*, "XXVII Fide Congress" 2016, vol. 32.

[33] A. Pim, B. Pascal, J.- F. Bohnert, M. Böse, P. Langbroek, A. Renier, T. Wahl, *Towards a Common Evaluation Framework to Assess Mutual Trust in the Field of EU Judicial Cooperation in Criminal Matters*, March 2013, https://www.government.nl/binaries/government/documenten/reports/2013/09/27/short-version-of-the-final-report-towards-a-common-evaluation-framework-to-assess-mutual-trust-in-the-field-of-judicial-coopera/j-19875-web-samenvatting-engels-bhoendie.pdf (access: 12.12.2024), p. 15.

[34] All the instruments indicated here govern the cross-border cooperation with the Member States of the Union. Additionally, to the package are the Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63/1, 6.3.2002), Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) (OJ EU L 135/53, 24.5.2016), and Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams (OJ L 162/1, 20.6.2002).

[35] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ EU L 130/1, 1.5.2014).

gathering of the data in a cross-border context within the Member States.[36] On the other hand, when in the context of cross-border evidence exchange with non-EU countries was supported by the Agreement on Mutual Legal Assistance MLA.[37]

Additionally, recent developments, such as the CLOUD Act (Clarifying Lawful Overseas Use of Data Act) have changed how countries share data across borders. This U.S. law allows the U.S. and other countries to exchange electronic data for criminal investigations, bypassing the MLA procedure. Though the CLOUD Act mainly affects the U.S. law enforcement, it also influences international agreements and data protection rules around the world.[38]

Given the volatile nature of electronic evidence which could not be supported in a timely manner due to the lengthy procedures of the MLA, instead of amending the European Investigation Order, the Council of the European Union proceeded with the establishment of Regulation 2023/1543/EU on European Production Orders (EPOs) and European Preservation Orders (EPrOs) for electronic evidence in criminal proceedings.[39]

Established on the grounds of Article 82 (1) TFEU and in compliance with the principles of subsidiarity and proportionality,[40] the Orders lays down rules and procedures on handling of the three types of electronic evidence: subscriber data, traffic data and content data.[41] The Orders are composed of binding rules empowering

[36] Article 3 of Directive 2014/41/EU defines the scope of the European Investigation Order application, clearly defining the scope of the carrying of the investigative measures between the Member States of the European Union.

[37] Two notably MLAs include the Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America (OJ EU L 291/40, 7.11.2009) and Council Decision 2010/616/EU of 7 October 2010 on the conclusion of the Agreement between the European Union and Japan on mutual legal assistance in criminal matters (OJ EU L 271/3, 15.10.2010).

[38] In 2023, the U.S. Department of Justice and the European Commission announced the resumption of negotiations on an agreement between the EU and the U.S. aimed at making it easier to access electronic evidence for criminal investigations. The full text of the CLOUD Act is available at https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf (access: 12.12.2024).

[39] European Commission, in its addressing of the proposal for the new instrument to allow the gathering of e-evidence with non-EU members, specified that EPPOs would constitute a better alternative than the amending of the European Investigation Order Directive in acknowledgement of the pellicular challenges in obtaining electronic evidence. See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, Strasbourg, 17.4.2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225 (access: 12.12.2024).

[40] Council of Europe, *Joining the Convention on Cybercrime…*; Council of Europe, *The Budapest Convention on Cybercrime…*

[41] The categorization of the evidence within the EU framework, aligns with the provisions by the Budapest Convention and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic

law enforcement authorities in the EU to order a third party[42] to generate or retain electronic evidence in a transnational exchange of data. The EPOs' new approach to criminal justice does not involve the intercession of foreign state authorities and prioritizes the operational base of the private entity over the data storage location, introducing a new height of mutual recognition principle, surpassing traditional judicial cooperation.[43] The Regulation 2023/1543/EU has faced criticism from both academia and professionals regarding its (i) legal applicability of Article 82 (1) TFEU stipulating judicial cooperation in the matter,[44] and (ii) the removal of the traditional principle of dual criminality.[45] In addition, critical studies on the EPOs and EPrOs argue that these instruments limit legal remedies, as the EPrO secures data without allowing immediate access, and the EPO only permits review after formal data request, interfering with timely legal action.[46] Another issue highlighted is the conflict of interest for service providers, who must balance cooperation with law enforcement while protecting user privacy and business interests, leading to concerns about how personal data is shared.[47] Furthermore, it is argued that the lack of uniformity regarding the admissibility of the electronic evidence obstructs cross-border criminal prosecutions and undermines the effectiveness of international cooperation in addressing global crime.[48]

The protection of personal data in the EU data gathering instruments composed by the EPOs is safeguarded by the Data Protection Acquis, composed by General

communications sector (OJ EU L 201/37, 31.7.2002). The provisioning of the type of data subjected to the Regulation subject matter are lied in Recital 31 of Directive 2002/58/EC.

[42] The service provider is to be offering its services within the jurisdiction of European Union.

[43] T. Wahl, *Commission Proposes Legislative Framework for E-Evidence*, "Eucrim" 2018, no. 1, pp. 35–36. The author argues that EPOs allows for authorities to require data from service providers operating within EU, irrespective of the location of the data, present such a new approach to the co-operation within criminal procedure shifting away from the traditional paradigm. See European Data Protection Board, *Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Art. 70.1.b)*, 26.9.2018, https://www.edpb.europa.eu/sites/default/files/files/file1/eevidence_opinion_final_en.pdf (access: 12.12.2024).

[44] See Council of Bars and Law Societies Europe, *CCBE Position on the Commission Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, 19.10.2018, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf (access: 12.12.2024); European Data Protection Board, *Opinion 23/2018 on Commission Proposals…*

[45] P. Topalnakos, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, "Eucrim" 2023, no. 2, p. 202.

[46] *Ibidem*.

[47] A. Juszczak, E. Sason, *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence*, "Eucrim" 2023, no. 2.

[48] L. Bachmaier, *Mutual Admissibility of Evidence and Electronic Evidence in the EU: A New Try for European Minimum Rules in Criminal Proceedings?*, "Eucrim" 2023, no. 2.

Data Protection Regulation (GDPR) and the Directive 2016/680/EU on Data Protection for Police and Criminal Justice Authorities. Providing context to the mutual trust framework in accordance with Article 82 TFEU, central to the architecture of the cooperation based on mutual recognition has been the enforcement by all Member States of the ECHR, and in post-Lisbon Treaty binding adherence to the European Charter of Fundamental Rights.[49] In particular, Article 7 ("Respect for Private And Family Life") and Article 8 ("Protection of Personal Data") of the Charter, alongside Article 8 ECHR ("Right to respect for private and family life"), establish fundamental grounds for legitimizing the access to and processing of personal data, in balance with the public interest. Whilst the mutual trust framework has brought in profound changes in the Union in terms of guaranteeing data protection, relevant stakeholders have raised concerns regarding human rights safeguarding, given the diverse legal traditions of states.[50] Specifically, Regulation 2023/1543/EU has raised concerns on personal data implications in the light of the lack guarantees on providing legal remedies within the enforcing state.[51]

2. A case study of Albania

2.1. Compliance with the Council of Europe framework

Pursuant to Law No. 8888 of 25 April 2002, the Parliament of the Republic of Albania ratified the framework of the Budapest Convention, whereas it emphasizes the responsibility to adopt a compliant legal framework.[52] Following the ratification process, amendments were proceeded in the national criminal substantive and criminal procedural law, pertaining Law No. 10023 of 27 November 2008 "On some additions and amendments to Law No. 7895 of 27 January 1995 Criminal Code of Republic of Albania, amended" and Law No. 10054 of 29 December 2008 "On some amendments to the Criminal Procedural Code, amended".[53] Namely,

[49] S. Carrera, F. Geyer, *The Reform Treaty and Justice and Home Affairs – Implications for the Common Area of Freedom, Security and Justice*, "Centre for European Policy Studies" 2007, vol. 141.

[50] E. Brouwer, *Mutual Trust and Human Rights in the AFSJ: In Search of Guidelines for National Courts*, "European Papers" 2016, vol. 1, pp. 893–920; A. Rosanò, *op. cit.*, p. 9.

[51] In its Opinion 7/2017 EDPS, whilst supporting the EPOs, highlights that the instrument should abide and fully respect the Charter of Fundamental Rights of the EU. See European Data Protection Board, *Opinion 7/2019: EDPS Opinion on Proposals Regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, 6.11.2019, https://www.edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf (access: 12.12.2024).

[52] The text of the Law in Albanian is available at https://qbz.gov.al/eli/ligj/2002/04/25/8888 (access: 14.12.20240).

[53] The amendments to criminal law introduced eleven new offences concerning crimes committed in cyberspace, aligning with the framework outlined in the Budapest Convention. Furthermore,

the updated criminal procedural provisions govern the management of computer data throughout the chain of custody process. These provisions include regulations for the production and sequestration of electronic evidence (detailed in Articles 191/a and 208/a of the Criminal Procedural Code) as well as the preservation phase (addressed in Articles 299/a and 299/b of the Criminal Procedural Code).[54] Additionally, further amendments[55] to the procedural law stipulated the preservation and administration of data in criminal proceedings; whilst the limits, authorization and procedure regarding communication interception were further regulated by Law No. 35/2017 "On several changes and additions to law No. 7905 of 21 March 1995 Code of Criminal Procedure of Albania".[56] Albania signed in 2021 Second Additional Protocol to the Budapest Convention, yet has not proceeded with its ratification. Currently, the cross-border exchange of electronic evidence is carried out based on MLA as stipulated in the Budapest Convention in the judicial cooperation in the field of criminal law, where judicial authorities are involved in validating the request and providing collection of the evidence. Considering the lengthy procedures and volatile nature of e-evidence, Albania has approached to police-to-police cooperation as an alternative to MLA.[57]

Accordingly, national legislation has been adopted, to provide data protection safeguards in the criminal procedure, with special regard to the evidence processing. Domestic framework on the matter is enshrined in the light of the ECHR,[58] and pursuant to Article 5 of the Constitution of the Republic of Albania (RoA) of 21 October 1998[59] binding international law is applicable in the country's jurisdiction. The integration of the rights and obligations deriving from Article 8 ECHR

---

the criminal procedural law now incorporates four new articles governing computer data and the collection of electronic evidence. The analysis of the amendments to the law have been researched by the author. See G. Cami, *Administration of Electronic Evidence in Criminal Proceedings: Regulatory Framework in Albania*, "Journal of International Institute for Strategic Research International Students. Interdisciplinary Scientific Conference Papers" 2023.

[54] Criminal Procedural Code of Albania of 21 March 1995. English translation of the Act is available at https://legislationline.org/sites/default/files/documents/97/Albania_CPC_1995_am2017_en.pdf (access: 12.12.2024).

[55] These changes in the criminal procedure were introduced by Law No. 9918/2008 "On electronic communication", introducing accordingly Article 101 of the Criminal Procedural Code.

[56] The Law introduced the new provisions corresponding to Articles 221 to 223 of the Criminal Procedural Code.

[57] Council of Europe, *Assessment Report on Obtaining and Using Electronic Evidence in Criminal Proceedings Under Domestic Legislation in South-Eastern Europe and Turkey*, 5.3.2018, https://rm.coe.int/3156-52-iproceeds-electronic-evidence-report-eng/16807bdfdf (access: 10.12.2024), see data on Albania.

[58] Convention for the Protection of Human Rights and Fundamental Freedoms was ratified by Albania in 1996 by the means of Law No. 8137 of 31 July 1996.

[59] English translation of the Constitution is available at https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)064-e (access: 10.12.2024).

into national law is ensured through the following safeguards provided by Albanian legislation:

1. Constitution of RoA. Article 15 of the Constitution guarantees the protection of fundamental human rights, which form the basis of the juridical order in the country. It further asserts that these rights and freedoms are indivisible, inalienable and inviolable. Furthermore, Article 35 ensures individual consent as a safeguard for the collection and usage of personal data, affirming individuals' right to be informed about data collected about them. This is further supported by Article 36, which ensures the right to privacy and the protection of personal data, and by Article 42, which safeguards the right to access justice and to seek legal remedies, ensuring that any violation of these fundamental rights can be addressed through the court.
2. Data Protection Law. In Albania, personal data processing legal framework is governed by Law No. 9887 of 10 March 2008 "On protection of personal data".[60] The legal act asserts that the right to privacy shall be guaranteed by law and handled with due regard for fundamental rights and freedoms. In accordance with Article 35 of the Constitution of RoA, it requests personal consent, as a pre-requisite for data processing of his persona[61] and reserves the right to request legal contest should data be collected in violation of the law. The principle of necessity in processing personal data is outlined in Article 5 (b) (c) of the Law, ensuring that any data processing remains within the bounds of its intended purpose. With specific reference to criminal proceedings, Article 6 (2) allows the Controller to process personal data in the context of crime prevention and prosecution activities, criminal offences against public order, other offences as provisioned by the substantive law. According to the provisional norms established in this Law, Albanian legislation of data protection legitimates with power to process data only bodies that either are established in the territorial jurisdiction of Albania or extra-territorial bodies, under the condition that they make use of any equipment located in RoA. Shall the Second Protocol be ratified by Albania, the current law will have to undergo amendment in the means of its Article 6 (2) to empower extraterritorial processors with the legitimacy to process personal data of Albanian citizen, given that national authorities shall not be involved in the collection of data directly from service providers. However, Article 8

[60] The Law has been amended twice, respectively through Law no. 48/2012 "On some additions and changes to the Law no. 9887 of 10 March 2008 On the protection of personal data of 8 May 2012", and Law no. 120/2014 "On some additions and changes to the Law no. 9887 of 10 March 2008 On the protection of personal data of 18 September 2014".

[61] See Article 6 (a) (a) of the Law No. 9887.

of the Law allows for the international transfer of the data, if the recipient state has an adequate level of personal data protection.

3. Criminal Procedural Code of the RoA.[62] Article 8/a makes specific reference to the processing of evidence in the criminal proceedings, emphasizing that such handling must not infringe upon human rights and fundamental freedoms.[63]
4. Albanian case law. The Supreme Court of Albania, through decision No. 147/2021 offered a legal analysis on the balance between data privacy and public security, through the interpretation of the principles of necessity, proportionality and appropriateness during the seizure of e-evidence.[64] The decision is considered a unified practice in the judiciary, and serves as a binding interpretive norm for the cases to be.

2.2. Approximation with the EU *acquis*

Albania started its commitment toward EU membership since early 2000s, and currently has been granted the candidate status. Pursuant to Article 70 of the Stabilization and Association Agreement (SAA),[65] Albania is required to approximate its domestic law with *acquis communautaire*.[66] In this context, legislation harmonization process is to guarantee alignment between existing and forthcoming laws with the Community *acquis*, ensuring proper enforcement.[67] Specifically, Article 85 SAA provides with the cooperation between Albania and European Union in the field of criminal matters, specifically addressing such cooperation in the combatting of

[62] Criminal Procedural Code of RoA has been subjected to 18 amendments by Law, between 1995–2017.

[63] This guarantee was added to the Criminal Procedural Code by Law 35/2017 "On some additions and amendments to the Law no. 7905 of 21 March 1995 Criminal Procedural Code of Albania", Article 6 of Law 35/217 scope was to harmonize its provisions with the best international standards and jurisprudence of European Court of Human Rights.

[64] Judgment of the Supreme Court of Albania of 21 December 2021, No. 22, case *Lapsi.al, Bushati & Shkullaku*.

[65] Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Albania, of the other part (OJ EU L 107/166, 28.4.2009), signed in 2006, and effective as of 1 April 2009, is the core document supporting the integration process toward EU membership. It constitutes the framework of relations between Albania and EU, and acts as the backbone structure to implement the accession process.

[66] The process of European integration is governed by National Plan for the Implementation of the Stabilization and Association Agreement (NPISAA). This document is drafted and implemented by the Ministry of Foreign Affairs (Albania), and the version subjected to the analysis in the 2022–2024 edition (https://integrimi-ne-be.punetejashtme.gov.al/wp-content/uploads/2022/02/NPEI_2022-2024_EN-.pdf).

[67] The SAA has been approved in Albania by its Law No. 9590 of 27 July 2006 "On the ratification of the Stabilization and Association Agreement between the Republic of Albania and the European Communities of their member states".

cybercrimes. Furthermore, Article 70 SAA stipulates the requirement for aligning national legislation concerning protection of personal data with both Community law and relevant international legislation on the privacy. Though Albania is not yet a Member State of the European Union, such provisioning aims for Albania legislator to guarantee adhering with the principles and standards of the *acquis communautaire*.

Presently, research examining the compliance of electronic evidence regulations with international law, solely references jurisprudence from the European Court of Human Rights, without incorporating the legal standards set forth in the EU *acquis*, including interpretations from the European Court of Justice. This methodology is supported by the assertion that, due to the country's non-EU status, the law prohibits considering arguments in accordance with the EU *acquis*.

In contrast to current practice, this study argues that any research conducted on the Albanian substantive and procedural law governing cybercrimes and/or electronic evidence, should include references to the *acquis communautaire*. This is particularly relevant given that Albania, alongside with EU Member States has adopted the same legislation for regulating crimes committed in cyberspace, as governed by the Budapest Convention and its Additional Protocols. Therefore, when assessing the compliance, consistency and stability of the national law with international law, it is useful to include analysis of EU legislation comprising legal acts, laws and court decisions related to the subject matter. Incorporating the comparative analysis references from EU law would provide appropriate learning experience for jurisprudence and legal interpretations conducted in the research.

In fact, the Constitution of RoA provides the prelacy of legal norms deriving from international law pursuant to the agreements between the RoA and the international organization, when conflict of interest arises over the applicability of law.[68] Such constitutional position contemplates the role of the EU in the Albanian legal framework, in reference to the SAA ratified since 2009. The Constitutional Court of Albania in its judgment No. 30 of 17 June 2010 addresses standards deriving from the European Court of Justice and additionally refers to the Council of Europe, Committee of Minister Resolution (75) 11 on the Criterial Governing Proceedings Held in the Absence of the Accused.[69] Furthermore, the Supreme Court of Albania, pursuant to its decision No. 22/2011 addresses respectively Article 31 of the Council Regulation (EC) No. 44/2001 on Jurisdiction and on Recognition and Enforcement of Judgments in Civil and Commercial Matter, and further recognizes the role of the EU law as a guidance for Albanian legal practice.[70]

[68] Congruent to Article 122 (3) and Article 123 of the Constitution, international law ratified by the Albanian legislator has prevalence on the national law on the subject matter.

[69] Judgment of the Constitutional Court of Albania of 17 June 2010, No. 30, paras 26 and 27 of the discussion.

[70] Judgment of the Supreme Court of Albania of 20 January 2011, No. 1.

Likewise, scholars in Albania emphasize the relevance and significance of referral to the EU law, advocating that a proper implementation of the *acquis* requires for the Albanian judiciary to assess national law based on EU standards within the EU *acquis*.[71]

CONCLUSIONS

The regulation of cross-border collection of electronic evidence has become of central importance within both international and European law. Acknowledging the need for enhanced regulations to facilitate international cooperation in criminal justice, the Council of Europe and the European Union have remedied the legal framework through the establishment of respective instruments. The study draws attention to the complex interplay between law enforcement operational framework and human rights considerations with regard to the data protection safeguards in the realm of cross-border access to electronic evidence within criminal proceedings.

Substitution of the MLA tool, with the new procedural powers contained within the Second Additional Protocol and Regulation 2023/1543/EU provides law enforcement authorities with more streamlined means to access data directly from service providers. This has allowed criminal justice to bypass the lengthy procedures through the involvement of national authorities, providing more effective transnational collaboration in criminal proceedings. The processing of electronic evidence vis-à-vis the new tools has been subjected to careful considerations in regard to the powers delegated to stakeholders in the process and personal data protection, ensuring alignment of new procedural powers with the guarantees deriving from the ECHR and EU Charter on Fundamental Rights.

Acknowledging the efforts of the legislator to establish safeguards, challenges still persist, notably in (i) balancing law enforcement requirements with privacy protections, (ii) new procedural powers potentially may exceed the scope of Article 82 TFEU by enhancing international cooperation beyond judicial authorities, and (iii) concerns regarding privatization of justice by granting service providers judicial authority. Particularly, in terms of data protection considerations during the cross-border collection of electronic evidence, the varying frameworks across countries, each with different levels of safeguarding, significantly impact the data of citizens involved in the process.

The case study of Albania provides insights from the perspective of compliance and implementation of these frameworks. While legislation has been aligned

[71] E. Muharremaj, *The Role of Legislation and Courts in the Protection of the Environment in the European Union and Its Impact on the European Integration of Albania*, "elni Review" 2018, no. 1, pp. 14–16.

with the Council of Europe framework, insights shared by stakeholders in criminal justice confirm that MLA provides with lengthy procedures and timeframes that do not comply with the volatile nature of the electronic evidence. A facilitated cross-border collaboration through the means of the Second Additional Protocol is considered to be a remedy for a more effective justice; however, national data protection laws require review and reinforcement to establish a high-standard framework. Despite not being a member state of the EU yet, the paper addresses the importance of referencing and relying on EU legislation and European Court of Justice jurisprudence in both judicial interpretations at the national level and in academia. This approach would further enhance harmonization of the domestic law with *acquis communautaire* and ensure a more comprehensive implementation of international standards.

REFERENCES

Literature

Bachmaier L., *Mutual Admissibility of Evidence and Electronic Evidence in the EU: A New Try for European Minimum Rules in Criminal Proceedings?*, "Eucrim" 2023, no. 2, **DOI: https://doi.org/10.30709/eucrim-2023-019**.

Brouwer E., *Mutual Trust and Human Rights in the AFSJ: In Search of Guidelines for National Courts*, "European Papers" 2016, vol. 1.

Cami G., *Administration of Electronic Evidence in Criminal Proceedings: Regulatory Framework in Albania*, "Journal of International Institute for Strategic Research International Students. Interdisciplinary Scientific Conference Papers" 2023.

Carrera S., Geyer F., *The Reform Treaty and Justice and Home Affairs – Implications for the Common Area of Freedom, Security and Justice*, "Centre for European Policy Studies" 2007, vol. 141.

Carrera S., González Fuster G., Guild E., Mitsilegas V., *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, Brussels 2015.

De Busser E., *The Digital Unfitness of Mutual Legal Assistance*, "Security and Human Rights" 2018, vol. 28(1–4), **DOI: https://doi.org/10.1163/18750230-02801008**.

Juszczak A., Sason E., *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice: An Introduction to the New EU Package on E-evidence*, "Eucrim" 2023, no. 2, **DOI: https://doi.org/10.30709/eucrim-2023-014**.

Karagiannis C., Verdigis K., *Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal*, "Information" 2021, vol. 12(5), **DOI: https://doi.org/10.3390/info12050181**.

Karsai K., *Division of Competences between Member States and the European Union in Criminal Procedural Law*, "XXVII Fide Congress" 2016, vol. 32.

Mitsilegas V., *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence*, "Maastricht Journal of European and Comparative Law" 2018, vol. 25(3), **DOI: https://doi.org/10.1177/1023263X18792240**.

Muharremaj E., *The Role of Legislation and Courts in the Protection of the Environment in the European Union and Its Impact on the European Integration of Albania*, "elni Review" 2018, no. 1, **DOI: https://doi.org/10.46850/elni.2018.003**.

Rosanò A., *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le proposte della Commissione europea sugli ordini di produzione e convervazione di prove elettroniche (e-evidence)*, "La Legislazione Penale" 2020.

Topalnakos P., *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, "Eucrim" 2023, no. 2, **DOI: https://doi.org/10.30709/eucrim-2023-015**.

Tosza S., *Gathering Electronic Evidence for Administrative Investigations*, "Eucrim" 2023, no. 2, **DOI: https://doi.org/10.30709/eucrim-2023-018**.

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, New York 2013.

Wahl T., *Commission Proposes Legislative Framework for E-Evidence*, "Eucrim" 2018, no. 1.

Online sources

AccessNow, *Access Now's Comments on the Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*, 30.4.2021, https://rm.coe.int/0900001680a25783 (access: 12.12.2024).

Alimonti V., *Assessing New Protocol to the Cybercrime Convention in Latin America: Concerns, Human Rights Considerations, and Mitigation Strategies*, 2022, https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam.pdf (access: 10.12.2024).

Council of Bars and Law Societies Europe, *CCBE Comments on the Draft 2nd Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*, 30.4.2021, https://rm.coe.int/0900001680a25786 (access: 10.12.2024).

Council of Bars and Law Societies Europe, *CCBE Position on the Commission Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, 19.10.2018, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf (access: 12.12.2024).

Council of Europe, *Assessment Report on Obtaining and Using Electronic Evidence in Criminal Proceedings Under Domestic Legislation in South-Eastern Europe and Turkey*, 5.3.2018, https://rm.coe.int/3156-52-iproceeds-electronic-evidence-report-eng/16807bdfdf (access: 10.12.2024).

Council of Europe, *Joining the Convention on Cybercrime: Benefits*, 8.2.2024, https://rm.coe.int/cyber-buda-benefits-8-february-2024-en-2776-0534-0937-v-1/1680ae70ee (access: 10.12.2024).

Council of Europe, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, https://rm.coe.int/16802e726c (access: 10.12.2024).

Council of Europe, *The Budapest Convention on Cybercrime: Benefits and Impact in Practice*, Strasbourg, 13.7.2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (access: 10.12.2024).

Council of Europe, *Worldwide Capacity Building*, https://www.coe.int/en/web/cybercrime/capacity-building-programmes (access: 12.12.2024).

Cybercrime Programme Office of the Council of Europe, *Standard Operating Procedures for the Collection, Analysis and Presentation of Electronic Evidence*, 12.9.2019, https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb (access: 10.12.2024).

European Commission, *Frequently Asked Questions: New EU Rules to Obtain Electronic Evidence*, 17.4.2018, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345?gclid=CjwKCAiA_aGuBhACEiwAly57McBWp6fAuIri3Hwc9lsVHVNHRqij3Bdz5kERTjzM_R-YrNvy19l6BRoCND4QAvD_BwE (access: 12.12.2024).

European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, Strasbourg, 17.4.2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX-:52018PC0225 (access: 12.12.2024).

European Data Protection Board, *EDPB Contribution to the 6th Round of Consultations on the Draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime*, Brussels, 4.5.2021, https://rm.coe.int/0900001680a26108 (access: 12.12.2024).

European Data Protection Board, *Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Art. 70.1.b)*, 26.9.2018, https://www.edpb.europa.eu/sites/default/files/files/file1/eevidence_opinion_final_en.pdf (access: 12.12.2024).

European Data Protection Board, *Opinion 7/2019: EDPS Opinion on Proposals Regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, 6.11.2019, https://www.edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf (access: 12.12.2024).

Jones N., George E., Mérida F.I., Rasmussen U., Völzow V., *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges*, Strasbourg 2019, https://rm.coe.int/0900001680a22757 (access: 10.12.2024).

Pim A., Pascal B., Bohnert J.-F., Böse M., Langbroek P., Renier A., Wahl T., *Towards a Common Evaluation Framework to Assess Mutual Trust in the Field of EU Judicial Cooperation in Criminal Matters*, March 2013, https://www.government.nl/binaries/government/documenten/reports/2013/09/27/short-version-of-the-final-report-towards-a-common-evaluation-framework-to-assess-mutual-trust-in-the-field-of-judicial-coopera/j-19875-web-samenvatting-engels-bhoendie.pdf (access: 12.12.2024).

Legal acts

Constitution of the Republic of Albania of 21 October 1998.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981, ETS No. 108.

Convention on Cybercrime, Budapest, 23.11.2001, ETS No. 185.

Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63/1, 6.3.2002).

Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America (OJ EU L 291/40, 7.11.2009).

Council Decision 2010/616/EU of 7 October 2010 on the conclusion of the Agreement between the European Union and Japan on mutual legal assistance in criminal matters (OJ EU L 271/3, 15.10.2010).

Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams (OJ L 162/1, 20.6.2002).

Criminal Procedural Code of Albania of 21 March 1995.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ EU L 201/37, 31.7.2002).

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ EU L 130/1, 1.5.2014).

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) (OJ EU L 135/53, 24.5.2016).
Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ EU L 191/118, 28.7.2023).
Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Strasbourg, 12.5.2022, CETS No. 224.
Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Albania, of the other part (OJ EU L 107/166, 28.4.2009).

Case law

Judgment of the Constitutional Court of Albania of 17 June 2010, No. 30.
Judgment of the Supreme Court of Albania of 20 January 2011, No. 1.
Judgment of the Supreme Court of Albania of 21 December 2021, No. 22.

ABSTRAKT

Wraz z rozwojem techniki teleinformatycznej oraz większej komputeryzacji w społeczeństwie wytwarzanie i przesyłanie danych coraz bardziej opiera się na przetwarzaniu w chmurze. Co za tym idzie znaczenie dowodów elektronicznych w postępowaniu karnym wzrasta, obejmując zarówno cyberprzestępczość, jak i przestępstwa tradycyjne. Zważywszy na ponadgraniczny charakter wymiany danych, ponadnarodowe regulacje i współpracę, zbieranie e-dowodów stanowi proces będący wyzwaniem dla postępowania karnego, zwłaszcza gdy wiąże się z konsekwencjami dla praw człowieka. Badając uregulowania prawne Rady Europy oraz Unii Europejskiej dotyczące postępowania z dowodami elektronicznymi, w artykule w szczególności oceniono procedury i zagadnienia prawne dotyczące wymiany danych elektronicznych w ramach różnych jurysdykcji w zakresie postępowania karnego. Skoncentrowano się głównie na doświadczeniach albańskich, obejmując analizą porównawczą przestrzeganie przez Albanię zasad w zakresie dowodów elektronicznych przy zapewnianiu zabezpieczeń w ramach ochrony danych w postępowaniu karnym.

Słowa kluczowe: przesyłanie danych; regulacje ponadnarodowe; jurysdykcje; postępowanie karne