JURNAL CITA HUKUM (Indonesian Law Journal)
FSH UIN Syarif Hidayatullah Jakarta
Vol.13 No. 2 (2025), pp. 605-618, DOI: 10.15408/jch.v13i2.46857

Legal Basis of Cross-Border Criminal Prosecution of Cybercriminals: Criminal and Procedural Challenges for Azerbaijan*

Shohlet Muzaffar Karimov,[1] Rashad Mammad Sharifov,[2] Akif Maharlam Eyvazov[3]
National Aviation Academy of Azerbaijan, Azerbaijan

10.15408/jch.v13i2.46857

Abstract
The impact of modern digital technologies is essential for understanding the need to improve the law enforcement system. The purpose of this article is to examine the legal basis for cross-border criminal prosecution of cybercrime in Azerbaijan, identify key criminal law and procedural challenges, and develop recommendations to improve national legislation and strengthen international cooperation. The study is based on an analysis of Azerbaijan's criminal and criminal procedure legislation in the field of cross-border prosecution of cybercrimes. Normative and comparative legal analysis methods, along with systematization, were employed to identify gaps and formulate recommendations. The results show that the Criminal Code of Azerbaijan contains references to the illegality of unauthorized access to computer information, illegal actions related to the exploitation of computer networks, and the distribution of malicious software. There is no separate article on computer fraud, so clear standards for collecting electronic evidence are not specified, indicating significant gaps in the national legal framework. The main challenges in cross-border prosecution of cybercrimes include the limited scope of bilateral extradition agreements, difficulties in cooperating with countries with different legal systems, and bureaucratic obstacles to the exchange of digital evidence. The conclusions highlight recommendations that would improve the regulatory framework. First and foremost, they call for implementing regulations on computer fraud and clear rules for the use of electronic evidence, expanding international cooperation, and implementing the provisions of international conventions to which Azerbaijan is a party.
Keywords: Cybercrime; Cross-Border Prosecution; Electronic Evidence; International Cooperation; Criminal Law of Azerbaijan

* Received: January 11, 2025, revised: March 12, 2025, accepted: June 22, 2025, Published: June 30, 2025.

[1] **Shohlet Muzaffar Karimov.** PhD in Law, Associate Professor at the Department of Law, Faculty of Economics and Law, National Aviation Academy of Azerbaijan. ORCID: https://orcid.org/0009-0008-5148-7898 Email: shkarimov@naa.edu.az

[2] **Rashad Mammad Sharifov.** PhD in Law, Senior Lecturer at the Department of Law, Faculty of Economics and Law, National Aviation Academy of Azerbaijan ORCID: https://orcid.org/0009-0001-8946-0403 Email: Rashadnauka2025@gmail.com

[3] **Akif Maharlam Eyvazov.** Senior Lecturer at the Department of Law, Faculty of Economics and Law, National Aviation Academy of Azerbaijan, Judge of the Court of Appeal, Chairman of the Judicial Board for Criminal Cases of the Shaki Court of Appeal of the Republic of Azerbaijan. ORCID: https://orcid.org/0009-0008-8767-7247 Email: akif.eyvazov@naa.edu.az

**Corresponding author: shkarimov@naa.edu.az

A. INTRODUCTION

Cybercrime is growing rapidly worldwide. This is due to the active development of digital technologies and the widespread introduction of information and communication systems in all areas of life. A distinctive feature of cybercrime is its cross-border nature; in particular, criminals operate from one country while causing harm to individuals or organizations in other countries (Caneppele & da Silva, 2022). The most common types of cybercrime include hacking, phishing, cyber fraud, and other misuse of information resources. The nature of these crimes poses challenges for national legal systems, especially for countries that are intensively developing their digital infrastructure. In addition, the study's relevance stems from the need to adapt Azerbaijan's criminal and procedural legislation to modern cross-border threats of cybercrime. As an active participant in international treaties, particularly the Budapest Convention on Cybercrime, Azerbaijan finds itself at the forefront of efforts to harmonize national legislation and strengthen international cooperation in this area (Macidov, 2023). At the same time, effective cross-border criminal prosecution of cybercriminals is complicated by several problems: jurisdictional conflicts, difficulties in extraditing suspects, challenges in collecting and securing digital evidence, and insufficient adaptation of national criminal and procedural norms to the realities of cross-border cybercrime. These challenges require a comprehensive analysis and the development of effective legal regulation mechanisms.

The purpose of this study is to analyse the legal basis for cross-border criminal prosecution of cybercrimes in Azerbaijan, identify key criminal law and procedural challenges, and formulate recommendations to improve national legislation and strengthen international cooperation. The research questions are as follows: 1. What are the key provisions of Azerbaijan's criminal and procedural legislation governing the prosecution of cybercrime? 2. How do international standards, particularly the Budapest Convention, influence the formation and development of Azerbaijan's national legal framework in the field of combating cybercrime? 3. What are the main problems in the practice of cross-border criminal prosecution of cybercrime, and what measures can contribute to the harmonization of legislation and the improvement of international cooperation?

Literature Review

The issue of cross-border criminal prosecution in cybercrime is actively discussed in academic literature, especially from the perspective of analyzing international legal doctrine. One of the key documents reflecting international

cooperation in fighting cybercrime is the Budapest Convention on Cybercrime (2001), developed and recommended by the Council of Europe. Some researchers, such as Ayoub (2024), Almanna (2023), and Dragojlović (2023), have examined the benefits of this instrument as a single, universal treaty. Although the document addresses both substantive and procedural aspects of combating cybercrime, there are skeptics regarding its implementation. Kastner (2021) argued that European legislative efforts are only successful within the EU, while other countries need to consider their local characteristics to build a truly effective legislative framework. Overall, several key issues emerge in scientific literature. The first is the challenge of jurisdiction in cyberspace, which has sparked significant debate over the legitimacy of prosecuting actions that affect multiple states (Casino et al., 2022; Franssen, 2024). The second issue concerns establishing principles for international cooperation, particularly in the areas of mutual legal assistance (MLA) and the extradition of suspects (Buçaj & Idrizaj, 2024). The third concerns the collection of electronic evidence. For example, research by Melossi (2020) and Shang (2023) highlights significant difficulties in verifying the authenticity and preserving the chain of evidence while adhering to procedural safeguards during digital evidence collection. The works of Chen (2024) and Nusa et al. (2025) focus on problems in applying the principle of territoriality in cyberspace. The researchers emphasized the need to find new approaches to jurisdiction, the "effects doctrine" principle. Research on UN cybersecurity decisions and the recommendations of the Budapest+ Initiative indicated a global demand to update existing international instruments (Ajoy, 2022). In the field of regional initiatives, it is important to analyze the EU Cybersecurity Strategy, which aims to harmonize legal approaches to the collection and transfer of digital evidence (e-evidence) (Russo & Stambøl, 2021). Researchers also examined the Council of Europe's projects to strengthen law enforcement agency capacity in the Eastern Partnership countries, including Azerbaijan. (Rzayeva, 2025)

The national and regional context of fighting cybercrime in Azerbaijan was also a key topic in scientific discussions. However, research on cross-border cybercrime remains limited. Some studies, such as Asgarova et al. (2022), address general aspects of combating cybercrime. However, a systematic analysis of the legal mechanisms for international cooperation in criminal prosecution has not been conducted. Scientific publications sometimes also fail to clearly distinguish between criminal law and criminal procedure aspects (AllahRakha, 2025). For comparison, it is helpful to consider the experiences of other CIS countries or the Asian region, where researchers mainly examine cybercrime from a technical and forensic perspective. For example, Macidov

(2023) and Kadir and Hartanto (2025), despite having limited practical relevance for Azerbaijani practitioners due to differing legal systems and political contexts, highlight general directions for developing strategies to combat cybercrime worldwide. Meanwhile, there has been a noticeable rise in scientific interest in cyberspace issues in China (e.g., Xue (2025)), although cross-border challenges remain a marginal topic. The proposed review has identified significant gaps in the scientific literature. Most scientific works analyze the challenges faced by developed countries with established legal cooperation mechanisms and digital infrastructure. The analysis of the specific legal problems of developing countries, particularly Azerbaijan, is insufficient. The challenges associated with adapting national criminal and procedural legislation to international standards, including procedural rights for suspects and access to electronic evidence, are not practically addressed. Similarly, specific recommendations for improving Azerbaijani legislation are rarely found in scientific literature. The lack of such recommendations, against the backdrop of ongoing developments in digital crime, underscores the need for further research that should primarily address the important task of harmonizing Azerbaijan's criminal procedure code with international standards.

B. METHODS

This study used a regulatory analysis method to determine the compliance of Azerbaijan's national legislation with the provisions of international treaties (the Budapest Convention and the standards of the Council of Europe and the UN). This enabled the effectiveness of national law in responding to the challenges of cross-border cybercrime. In addition, comparative legal analysis was used to compare Azerbaijani criminal law and procedural norms with the legislation of other countries, primarily EU countries (Estonia, Germany), which have significant experience in combating cybercrime at the international level. This allows us to identify best practices. At the same time, the systematization of legal provisions is used to structure norms, identify internal contradictions, gaps, or duplications in legal regulation, and formulate proposals to eliminate them.

The use of normative analysis is most appropriate for this study, as it enables us to focus on legal norms and their practical application in international cooperation. This approach is particularly relevant for Azerbaijan, as it allows the country to develop its digital infrastructure and join global cybersecurity mechanisms. At the same time, the comparison method provides insight into how legal challenges are addressed in other countries. It enables

their experience to inform the adaptation of Azerbaijan's legal system to international requirements.

C. RESULTS AND DISCUSSION

1. Analysis of Azerbaijani legislation

The development of digital technologies for cross-border interaction in cyberspace has created qualitatively new challenges for criminal law. Cybercrime, which knows no national borders, requires states to adapt their legislation to the conditions of the digital age and ensure practical international cooperation. For Azerbaijan, these issues are relevant due to the need to harmonize domestic legal norms with international standards and the provisions of the Budapest Convention on Cybercrime (Apsimet & Muratova, 2025). In this context, it is important to analyze the extent to which Azerbaijan's current criminal and criminal procedure legislation meets modern challenges in combating cybercrime, including cross-border criminal prosecution, the collection of electronic evidence, extradition, and mutual legal assistance. The Criminal Code of the Republic of Azerbaijan (Criminal Procedure Code of the Republic of Azerbaijan, 1999) contains several provisions that explicitly establish liability for cybercrimes (see Table 1).

Table 1.
Cybercrimes in the Criminal Code of the Republic of Azerbaijan

Article	Offenses	The essence of the offense
271	Access to computer information without proper authorization	The Criminal Code provides for liability for unauthorized penetration into computer systems for knowingly extracting, modifying or destroying data.
272	Violation of existing rules for operating a computer network	Sanctions are provided for intentional disruption of computer equipment or functioning networks.
273	Writing, using, and selling (any other distribution) of malicious software	The Criminal Code establishes penalties for specific actions involving the development or distribution of malicious computer programs.
178 (general)	Fraud	The general indication on fraud also provides for penalties for actions committed using information and communication technologies (ICT) and which can be qualified as computer fraud.

An analysis of the Criminal Code revealed that existing regulations are insufficient to combat the current level of digital crime. Given the ongoing development of digital technologies, Azerbaijan's criminal procedural legislation must continue to adapt to the challenges of today, including the investigation of cross-border cybercrimes and the prosecution of criminals. This area continues to be associated with significant legal gaps, which significantly complicate the effectiveness of the national criminal justice system. Separately,

it is worth noting other laws of the Republic of Azerbaijan that specify liability for criminal acts in the digital space. For a better understanding, the results are summarized in Table 2.

Table 2.
Cybercrimes in the legislation of the Republic of Azerbaijan

Law	Offenses	Essence of the offense
"On Personal Data", The Law No. №998-IIIQ (2010)	Illegal access to personal data	According to the analysis of the sources, there is no direct mention of the legal basis for cross-border criminal prosecution of cybercrimes. The source focuses on the legislation of the Republic of Azerbaijan regulating the collection, processing, and protection of personal data, as well as issues related to the formation of a national information space and cross-border transfer of personal data. The law governs cross-border transfers of personal data. Cross-border transfer of personal data is prohibited if it poses a threat to the national security of the Republic of Azerbaijan.
"On Requirements for the protection of personal data", Law (2010)	Violation of the protection of personal data	The legal source focuses on the "Requirements for the Protection of Personal Data" in Azerbaijan. It regulates relations related to the protection of personal data and relevant information systems during their collection, processing, dissemination, and transfer by the owner or operator of personal data.
"On the Prosecutor's Office", Law No. 767-IQ (1999)	Prosecutor's actions when working with digital evidence	The source mentions aspects that are quite indirectly related to modern technologies, without direct references to cyberspace. The General Prosecutor's Office of the Republic of Azerbaijan organizes the generalization of prosecutorial and investigative practice and the application of scientific and technical means to improve them and prevent offenses. This term is general and does not specify which scientific and technical means are used. The Prosecutor's Office also conducts operational and investigative activities to initiate criminal cases or investigate corruption-related crimes. The prosecutor also supervises the legality of conducting operational and investigative measures.

As established, existing legal practice in Azerbaijan allows the use of electronic evidence in criminal proceedings. However, the current Criminal Procedure Code does not contain explicit regulatory provisions regarding their legal status. For example, the legislation does not define the term "electronic evidence." There are no unified rules for collecting, seizing, and storing digital evidence, determining its authenticity, or using it in court proceedings. This situation has caused severe difficulties at the pre-trial investigation stage and during subsequent court proceedings. For example, there is a high legal risk that the defence will challenge the admissibility of electronic evidence (Stoykova, 2023). References to non-compliance with procedural requirements may well make it impossible to bring the guilty parties to justice. Law enforcement agencies often lack the necessary technical equipment to record

digital traces of crime (Widodo et al., 2024). The issue of sufficient qualifications to work with such evidence is an important area for further research.

2. Cross-border cooperation and international conventions

Azerbaijan actively cooperates with many other countries in the field of extradition, using multilateral international treaties. The most important in this context was the accession to the European Convention on Human Rights (1950), the European Convention on Data Protection (1981), and the European Convention on Mutual Assistance in Criminal Matters (1959). (also based on additional protocols, which are constantly being updated). However, this may not be sufficient to combat cybercrime effectively amid global digitalisation. For example, the lack of bilateral extradition agreements with many countries makes it significantly more challenging to detain or arrest suspects (Nieto Martín, 2021). This is particularly evident when working outside the CIS (including the US, Canada, and even some Asian countries). This fact significantly complicates access to suspects who are not under Azerbaijan's jurisdiction. This is further complicated by the fact that such countries are digital hubs, hosting key IT infrastructure nodes (servers, domain registrars, etc.) that are often used in cybercrime.

There are specific institutional barriers, including differences in legal systems, which create new additional obstacles to effective extradition (Mitgutsch, 2022). First, foreign jurisdictions require high standards of evidence and procedural guarantees that are not always available within the usual criminal proceedings in Azerbaijan. This situation creates additional obstacles against the backdrop of the refusal to extradite.

The functioning of specific mechanisms for the provision of mutual legal assistance primarily relies on international agreements. First, the process of exchanging information with foreign criminal law enforcement agencies remained lengthy and inconsistent. Unfortunately, the existing difficulties are particularly acute in the context of urgent preservation or even seizure of electronic data. Such evidence is significant but can be destroyed or altered in real time and within a relatively short period. Another challenge is the lack of fast automated procedures for the exchange of digital evidence, as explicitly stated in Articles 29–35 of the Budapest Convention (The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, 2005). Implementing this international treaty requires complex bureaucratic procedures.

Given that the Republic of Azerbaijan is a full member of the Budapest Convention (ratified in 2009), this instrument can be considered quite successful for the further development of international cooperation. The Criminal Code of Azerbaijan generally complies with the Convention's main criminal law provisions. First, it should be noted that Articles 271–273 of the Criminal Code are consistent with Articles 2–5 of the Convention, which allow for active cooperation in the field of combating unauthorized access to data, interception of important information, and interference with the functioning of digital systems (Criminal Procedure Code of the Republic of Azerbaijan, 2022). On the other hand, Azerbaijani legislation does not contain a separate provision on computer fraud, although the Budapest Convention requires such a provision under Article 8. Azerbaijani lawmakers also need to implement further provisions on the preservation and transfer of electronic data (as provided for in Articles 16–18 of the Convention). (The Convention on Cybercrime, (Budapest Convention, ETS No. 185) and its Protocols, 2005)

This study examines the legal foundations of cross-border cybercrime prosecution in Azerbaijan, focusing on key criminal law and procedural challenges. It analyzes how modern digital technologies create new demands for law enforcement and require stronger international cooperation. The research identifies key provisions in Azerbaijan's criminal legislation, highlights the influence of international standards such as the Budapest Convention on shaping national laws, and outlines major issues in cross-border enforcement. Finally, the study offers recommendations to improve national legislation and enhance collaboration between states in addressing the growing complexity of cybercrime.

The results indicate significant challenges in Azerbaijan's criminal law and criminal procedure systems in effectively combating cybercrime. Given its cross-border location, Azerbaijan may become a target for cybercriminals who can exploit loopholes in existing legislation and avoid punishment. The rapid growth of the digital economy in Azerbaijan has also increased the risks of unauthorized access to personal data, fraud, and the use of malicious software. The proposed results indicate that, despite the existence of specific criminal law provisions (e.g., Articles 271–273 of the Criminal Code), the legislation is limited in scope and does not cover the full spectrum of modern cyber threats. In this context, the results of the study confirm the conclusions of other studies (Corhay & Franssen, 2025). For example, according to de Arimatéia da Cruz (2020), legislative gaps in the regulation of electronic evidence and cross-border cooperation are direct conditions for the impunity of cybercriminals. Similar challenges have been identified in Eastern Partnership countries, where

international standards remain poorly integrated into national criminal procedure (Fernandes Godinho & Castro Marques, 2021). Similarly, AllahRakha (2024) noted that the lack of clear procedural rules for the use of electronic evidence is a significant barrier to the effective use of the Budapest Convention in practice. In addition, as established in the proposed results, the absence of the term "electronic evidence" in legislation is a clear marker of a trend that characterizes countries that are only in the process of adapting their legal framework to the international legal order. This coincides with the reservations proposed by Hert & Bouchagiar (2020). Therefore, without proper regulatory oversight, digital evidence is often the subject of appeals by the defense.

The proposed results indicate that, in practice, the country faces several serious challenges. Even Azerbaijan's tangible progress in establishing intergovernmental relations, primarily in the European Convention on Mutual Assistance in Criminal Matters (1959) and the ratified Budapest Convention on Cybercrime (2009), has little impact on this fact. The acute challenges lie in the limited number of bilateral extradition agreements and in institutional legal differences with other national jurisdictions. For example, compared to Turkey, which also ratified the Budapest Convention, Azerbaijan has demonstrated significantly less institutional capacity in data exchange. Turkey has implemented the provisions of Articles 16–18 of the Convention on the Preservation of Computer Data. In addition, Turkey has a well-developed infrastructure for promptly responding to requests from foreign partners. As Macidov (2023) noted in his study, Azerbaijan does not leverage the potential of interagency digital platforms, which could significantly speed up responses to international requests. Azerbaijan's criminal law still lacks a separate article on computer fraud, as required by Article 8 of the Budapest Convention. Turkey, on the other hand, updated its criminal code in 2016 to include the relevant offense. Also, as some studies have shown, in EU countries (such as Germany and France), tools for international cooperation on cybercrime are part of the European legal framework (Marcén, 2024). For example, with the approval of Europol or Eurojust, special task forces have been created capable of coordinating and exchanging information in real time (Wagner, 2020). In Azerbaijan, the exchange of necessary data is handled by traditional bureaucratic structures. This significantly hinders the implementation of Articles 29–35 of the Budapest Convention on international cooperation. The results also confirm the views of scholars who argue that technical or procedural barriers could hamper the actual implementation of the Budapest Convention's provisions in countries with limited digital resources. (Zhang & Gong, 2023)

By comparing the results with the recommendations of other scholars, it is possible to formulate specific proposals. The challenges identified thus confirm the need for further comprehensive codification of provisions on cybercrime (Nugman, 2023). Equally important is the ratification and further practical application of existing international legal instruments, including the Budapest Convention. Researchers highlight the need for deeper technical cooperation across borders and improved training for law enforcement officers (Zhang & Gong, 2023). Scientists also believe that in addition to the timely detection of unauthorized interference and the prevention of unauthorized interference, copying, and/or transfer of data to persons who are not authorized to work with it, advanced proactive threat monitoring systems can be implemented, such as intrusion detection and prevention systems (IDS/IPS) using machine learning to identify anomalous behavior (Gallant, 2022). Continuous monitoring of personal data protection is essential through independent pentests, vulnerability audits, and the use of licensed software. Implementing software whitelisting policies and conducting state examinations of data systems, along with annual protection audits, help strengthen security and reduce risks from unauthorized or malicious applications (Buçaj & Idrizaj, 2024). The powers of supervisory authorities to conduct unscheduled inspections in response to incidents or the discovery of significant new threats could be expanded, and more detailed methodologies for assessing compliance with security requirements could be developed.

The study's methodology has limitations that should be considered when interpreting the results. The comparative legal analysis focuses primarily on countries with a high level of digitalization (and, accordingly, legislative regulation). The study was conducted in accordance with the regulatory framework in force in 2024–2025. Legal regulation in the field of cybercrime is undergoing rapid transformation, so some of the legislative acts analyzed may change in the near future.

D. CONCLUSIONS

The results of the study show that the criminal and criminal procedure legislation of the Republic of Azerbaijan consists of several provisions aimed at combating cybercrime. First, this process is regulated by Articles 271–273 of the Criminal Code, which regulate illegal access to computer information, illegal actions related to the operation of computer networks, and the distribution of malicious software. However, as of today, there is no separate article on computer fraud, so clear standards for collecting electronic evidence are not specified, which indicates significant gaps in the national legal framework. The

main challenges in cross-border prosecution of cybercrimes stem from the limited number of bilateral extradition agreements. The challenges of cooperating with other jurisdictions with different legal systems, as well as bureaucratic obstacles to the exchange of digital evidence, complicate the prompt and effective investigation of crimes in the digital space.

This study makes a significant contribution by providing a comprehensive analysis of Azerbaijan's current legislation in relation to international standards, particularly the Budapest Convention. It offers concrete recommendations to enhance the national regulatory framework, including the adoption of norms on computer fraud and clear rules for the use of electronic evidence. Such measures would strengthen the effectiveness of Azerbaijan's criminal justice system and foster greater international cooperation in combating cybercrime. The proposed recommendations hold practical value for legislators, law enforcement agencies, and international partners. Furthermore, future studies should include empirical research on cybercrime prosecution practices and explore how emerging technologies—especially artificial intelligence and blockchain—affect the evolution of cybercrime and its legal regulation.

REFERENCES:

Ajoy, P. B. (2022). Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. *Scholars International Journal of Law, Crime and Justice*, *5*(2), 74–79. https://doi.org/10.36348/sijlcj.2022.v05i02.005

AllahRakha, N. (2024). Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. *International Journal of Law and Policy*, *2*(6), 1–9. https://doi.org/10.59022/ijlp.193

AllahRakha, N. (2025). Cross-Border E-Crimes: Jurisdiction and Due Process Challenges. *ADLIYA: Jurnal Hukum dan Kemanusiaan*, *18*(2), 153–170. https://doi.org/10.15575/adliya.v18i2.38633

Almanna, A. (2023). Cybercrime. In *Legal Translation between English and Arabic* (pp. 197–212). Springer International Publishing. https://doi.org/10.1007/978-3-031-14838-5_11

Apsimet, N., & Muratova, A. (2025). On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud. *Bulletin of the Karaganda University. "Law" Series*, *30*(1 (117)), 87–97. https://doi.org/10.31489/2025l1/87-97

Asgarova, M. P., Aliev, B. A., Khalilov, F. Y., & Hasanaova, I. Z. (2022). The use of electronic evidence in court: a comparative legal analysis in the world

practice. *Cuestiones Políticas*, *40*(72), 385–394. https://doi.org/10.46398/cuestpol.4072.21

Ayoub, L. (2024). Judicial Effectiveness or Judicial Ambiguity. In *Customary International Law and Its Interpretation by International Courts* (pp. 186–210). Cambridge University Press. https://doi.org/10.1017/9781009541312.008

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024. https://doi.org/10.31893/multirev.2025024

Caneppele, S., & da Silva, A. (2022). Cybercrime. In *Research Handbook of Comparative Criminal Justice* (pp. 243–260). Edward Elgar Publishing. https://doi.org/10.4337/9781839106385.00024

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, *8*(1), 1-18. https://doi.org/10.1093/cybsec/tyac014

Chen, Y. (2024). Research on E-discovery of Cross-border Cybercrimes. *Science of Law Journal*, *3*(7), 186-190. https://doi.org/10.23977/law.2024.030725

Corhay, M., & Franssen, V. (2025). Digital Evidence Gathering by US Authorities and Cross-Border Cooperation with US-Based Service Providers. In *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (pp. 569–586). Cambridge University Press. https://doi.org/10.1017/9781009049771.023

Criminal Procedure Code of the Republic of Azerbaijan, Code (2022) (Republic of Azerbaijan). https://e-qanun.az/framework/46950#_edn1

Dragojlović, J. (2023). Jurisdiction for criminal offenses of cybercrime: International and national standards. *Pravo - teorija i praksa*, *40*(suppl), 63–83. https://doi.org/10.5937/ptp2300063d

De Arimatéia da Cruz, J. (2020). The Legislative Framework of the European Union (EU) Convention on Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 223–237). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_5

Fernandes Godinho, I., & Castro Marques, N. (2021). Competition criminal law: an international and global trend? *SHS Web of Conferences*, *92*, 03011. https://doi.org/10.1051/shsconf/20219203011

Franssen, V. (2024). Cross-border gathering of electronic evidence in the EU: toward more direct cooperation under the e-Evidence Regulation. In *Research Handbook on EU Criminal Law* (pp. 184–211). Edward Elgar Publishing. https://doi.org/10.4337/9781800886438.00016

Gallant, K. S. (2022). The National and International Law of Criminal Jurisdiction. In *International Criminal Jurisdiction* (pp. 59–138). Oxford University Press. https://doi.org/10.1093/oso/9780199941476.003.0002

Hert, P. d., & Bouchagiar, G. (2020). Investigating Cybercrime and A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. *SCRIPT-ed*, *17*(2), 431–440. https://doi.org/10.2966/scrip.170220.431

Kadir, S. A., & Hartanto, H. (2025). Development of cybercrime and Indonesian criminal law. *Jurnal Meta-Yuridis*, *8*(1), 63–73. https://doi.org/10.26877/m-y.v8i1.20731

Kastner, P. (2021). International legal dimensions of cybercrime. In *Research Handbook on International Law and Cyberspace* (pp. 253–270). Edward Elgar Publishing. https://doi.org/10.4337/9781789904253.00022

Macidov, S. T. oglu (2023). Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations. *Futurity Economics&Law*, *3*(3), 78–94. https://doi.org/10.57125/fel.2023.09.25.05

Marcén, A. G. (2024). The Budapest Convention and the negotiations on the UN Cybercrime Convention. In *Global Cybersecurity and International Law* (pp. 174–192). Routledge. https://doi.org/10.4324/9781003344124-10

Melossi, D. (2020). The Connections between Migration, Crime and Punishment. In *Controlling Immigration Through Criminal Law*. Hart Publishing. https://doi.org/10.5040/9781509933952.ch-004

Mitgutsch, I. (2022). „International Criminal Law before Domestic Courts“ – Tagungsbericht. *Journal für Strafrecht*, *9*(1), 54-57. https://doi.org/10.33196/jst202201005401

Nieto Martín, A. (2021). The Ius Puniendi of International Organizations. In *Global Criminal Law* (pp. 17–48). Springer International Publishing. https://doi.org/10.1007/978-3-030-84831-6_2

Nugman, A. N. (2023). International legal regulation of the fight against cybercrime. *Deutsche internationale Zeitschrift für zeitgenössische Wissenschaft*, *65*, 11–13. https://doi.org/10.5281/zenodo.8414814

Nusa, I. Q., Sugiri, B., Yuliati, Y., & Sulistio, F. (2025). Law Enforcement of Cybercrime: Tracking Digital Footprints of Cross-Border Hackers. *International Journal of Islamic Education, Research and Multiculturalism (IJIERM)*, *7*(2), 776–802. https://doi.org/10.47006/ijierm.v7i2.475

"On data protection", Convention No. 108 (1981). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

"On Human Rights", Convention (1950). https://www.echr.coe.int/documents/d/echr/convention_ENG

“On Personal Data”, The Law No. №998-IIIQ (2010). (Republic of Azerbaijan). https://e-qanun.az/framework/19675

"On Requirements for the protection of personal data", Law (2010). (Republic of Azerbaijan). https://e-qanun.az/framework/20046#_edn1

“On the Prosecutor's Office”, Law No. 767-IQ (1999). (Republic of Azerbaijan). https://e-qanun.az/framework/5229#_edn1

Russo, A., & Stambøl, E. M. (2021). The external dimension of the EU's fight against transnational crime: Transferring political rationalities of crime control. *Review of International Studies*, 1–20. https://doi.org/10.1017/s0260210521000358

Rzayeva, G. A. (2025). International legal mechanisms for combating cybercrime: The economic impact on Azerbaijan and global practices. *Baltic Journal of Economic Studies*, *11*(1), 301–307. https://doi.org/10.30525/2256-0742/2025-11-1-301-307

Shang, L. (2023). Research on Cross-border Electronic Evidence Collection System. *Criminal Justice Science & Governance*, *4*(1), 31–39. https://doi.org/10.35534/cjsg.0401005

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, Convention (2005). https://www.coe.int/en/web/cybercrime/the-budapest-convention

Wagner, J. (2020). Frontex—The EU Border Management and Coast Guard Agency. In *Border Management in Transformation* (pp. 229–243). Springer International Publishing. https://doi.org/10.1007/978-3-030-62728-7_10

Widodo, M., Weiner, A. M., Zubaedah, P. A., Prayitno, A. H., & Andriani, F. (2024). International Legal Dynamics in Combating Cybercrime: Challenges and Opportunities for Developing Countries. *Global International Journal of Innovative Research*, *2*(1), 314–321. https://doi.org/10.59613/global.v2i1.49

Xue, C. (2025). The Potential Impact of Digital Currencies on Inflation in Developing Countries. *Advances in Economics, Management and Political Sciences*, *187*(1), 39–44. https://doi.org/10.54254/2754-1169/2025.bl23702

Zhang, H., & Gong, X. (2023). The research on an electronic evidence forensic system for cross-border cybercrime. *The International Journal of Evidence & Proof*, *28* (1), 21–44. https://doi.org/10.1177/13657127231187059