ADLIYA: Jurnal Hukum dan Kemanusiaan – ISSN: 1978-8312 (p), 2657-2125 (e)
Vol. 18, no. 2 (September 2024), pp. 153-170, doi: 10.15575/adliya.v18i2.38633

CROSS-BORDER E-CRIMES: JURISDICTION AND DUE PROCESS CHALLENGES

Naeem AllahRakha
Tashkent State University of Law, Uzbekistan

Correspondence Author: chaudharynaeem133@gmail.com

Received: 29 August 2024; Accepted: 30 September 2024; Published: 30 September 2024

Abstract
Cross-border e-crimes pose significant challenges due to the borderless nature of cyberspace and the complexities of international legal cooperation. This research examines the existing international legal frameworks, such as the Budapest Convention on Cybercrime, and their effectiveness in harmonizing laws and facilitating cross-border investigations. The study applies the doctrinal research methodology to analyze the regulations on cybercrimes. It analyzes the role of international standards of due process and prosecution in upholding individual rights and ensuring fair trials in cross-border cases. The legal frameworks for collecting and sharing digital evidence across borders are fragmented, creating significant challenges for international cooperation. Emerging technologies further complicate the governance of cybercrime. Law enforcement agencies face legal and privacy issues when accessing cross-border data stored in the cloud. The execution of mutual legal assistance requests in cybercrime cases remains slow and inefficient. Gaps in international frameworks hinder lawful access to electronic evidence, while cross-border cybercrime investigations experience delays due to language barriers, incompatible laws, and limited technical expertise within national agencies. These challenges underscore the need for a unified approach to tackle cross-border e-crimes effectively.

Keywords: *due process; e-crimes; jurisdiction; cross-border; legal frameworks*

Introduction

In an era where cybercriminals can breach data systems across continents in mere seconds, the question arises: whose laws should hold them accountable? The rise of cross-border e-crimes ranging from ransomware attacks to online fraud has created unprecedented challenges for jurisdiction and due process in the digital age. It is assessed that cybercrime will generate $8 trillion in revenue by the end of 2023 and $10.5 trillion in 2025, cybercrimes and victims scattered across different legal systems, the issue transcends national boundaries, demanding a global response.[1]

The borderless nature of cyberspace has rendered traditional jurisdictional boundaries increasingly porous, necessitating a robust international legal framework to address these emerging threats effectively. At the core of this challenge lies the tension between managing cyber risks, ensuring due process and prosecution standards, and addressing jurisdictional complexities. As businesses embrace digital

[1] Lena Klasén, Niclas Fock, and Robert Forchheimer, "The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age," *Forensic Science International* 362 (September 2024): 112133, https://doi.org/10.1016/j.forsciint.2024.112133.

technologies to drive growth and innovation, they must navigate a complex web of data protection laws and mitigate the risks of data breaches and cyber-attacks.[2]

The monitoring, investigation, and prosecution of cross-border e-crimes present unique hurdles. The decentralized and global nature of the internet complicates the collection and preservation of digital evidence, often spanning multiple jurisdictions.[3] Law enforcement agencies face the daunting task of tracing the origins of cyber-attacks and securing cooperation from various nations, each with its own legal frameworks and data protection regulations. International standards of due process and prosecution ensuring that cross-border investigations and prosecutions are conducted fairly and justly.

Enshrined in various international treaties and conventions, the standards emphasize the importance of a fair trial, the right to legal representation, and the protection of individual rights.[4] However, implementing the standards uniformly across different legal systems remains a significant challenge, exacerbated by the rapidly evolving nature of cybercrime and technology. The jurisdictional challenges posed by cross-border e-crimes are multifaceted.

The concept of territoriality, a cornerstone of traditional legal systems, is increasingly strained in the digital realm, where data and criminal activities transcend physical boundaries.[5] This has led to debates surrounding the appropriate jurisdictional tests and the extent to which nations can assert legal authority over digital activities that have cross-border implications. Efforts to address these challenges have been ongoing, with initiatives such as the Budapest Convention on Cybercrime serving as a foundational framework for harmonizing national laws and fostering international cooperation.[6]

Cybercrime jurisdiction is determined by factors like offender nationality and victim nationality. States may also establish jurisdiction based on impacts to national security. For instance, the protective principle allows states to protect vital interests. A connection must exist between the cybercrime and the state asserting jurisdiction. The United Kingdom applied this principle in *R v. Sheppard and Anor* (2010). Two UK residents were convicted under the UK Public Order Act. They posted racially inflammatory material on a US-hosted website, demonstrating extraterritorial

2 Saqib Saeed et al., "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors* 23, no. 15 (July 25, 2023): 6666, https://doi.org/10.3390/s23156666.

3 Moses Ashawa et al., "Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation," *Cloud Computing and Data Science* 5, no. 1 (December 25, 2023): 140–56, https://doi.org/10.37256/ccds.5120233845.

4 Lucia Zedner and Carl-Friedrich Stuckenberg, "Due Process," in *Criminal Justice and Procedure*, ed. Ambos Kai et al., vol. I (Cambridge University Press, 2019), 304–342.

5 Fuad Zubaidi, "Territoriality in the Traditional Context," *Psychology and Behavioral Sciences* 2, no. 3 (2013): 89, https://doi.org/10.11648/j.pbs.20130203.12.

6 David Wicki-Birchler, "The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?," *International Cybersecurity Law Review* 1, no. 1–2 (October 22, 2020): 63–72, https://doi.org/10.1365/s43439-020-00012-5.

jurisdiction. Similarly, Malaysia's Computer Crimes Act 1997 asserts jurisdiction over offences committed abroad. Article 9 ensures universal application regardless of location.[7]

Cybercrime creates significant jurisdictional challenges due to its complex, global nature. Conflicting jurisdictions arise when victims and perpetrators reside in different countries. The transnational aspect of cybercrimes involves individuals, systems, and activities across multiple legal territories. Evidence may be stored on servers located far from the crime scene. Websites hosted in one country but targeting users elsewhere complicate jurisdictional claims. Additionally, parts of a website might be distributed across various global locations. Traditional legal frameworks struggle to adapt to the intangible nature of cyberspace.[8]

The internet has fundamentally challenged traditional notions of due process in law. Identifying and prosecuting cybercriminals remains a complex and resource-intensive task. Cybercriminals exploit global networks and advanced technologies to obscure their activities effectively. Law enforcement agencies face difficulties in gathering admissible evidence across jurisdictions. Additionally, the internet facilitates the rapid spread of false information, often harming reputations irreparably. Online harassment, cyberbullying, and defamation have become prevalent societal issues. Legal systems have responded by enacting laws addressing cybercrimes and online misconduct.[9]

Government actions against cybercrimes often lead to violations of internet rights. A significant concern is the failure to secure search warrants, violating privacy. For instance, the United States proposed the Stop Online Piracy Act, promoting surveillance. This act faced public rejection for enabling online censorship practices. Another concern is entrapment, where authorities bait individuals into committing cybercrimes. Such practices raise constitutional questions regarding state-induced criminal activity. Additionally, cases like *Riley v. California* 573 U.S. 373 (2014), emphasize warrant requirements for phone searches.[10]

Recent research has delved into the complexities of cross-border cybercrime, particularly focusing on jurisdictional challenges and due process concerns. Legal frameworks for collecting and sharing digital evidence across borders are fragmented, creating significant challenges for international cooperation.[11] Emerging

---

7 F A Onomrerhinor Onomrerhinor, "Universal Jurisdiction For Transnational Cybercrimes?," *UCC Law Journal* 3, no. 1 (July 1, 2023): 119–51, https://doi.org/10.47963/ucclj.v3i1.1253.

8 Tripti Singh, "Cybercrime And International Law: Jurisdictional Challenges And Enforcement Mechanisms," *African Journal of Biomedical Research*, September 23, 2024, 697–708, https://doi.org/10.53555/AJBR.v27i3S.2101.

9 Giulia Gentile, "Between Online and Offline Due Process: The Digital Services Act," 2025, 219–38, https://doi.org/10.1007/978-3-031-65381-0_11.

10 Frank Chambers, "An Ongoing Seizure: The Struggle to Uniformly Protect Fourth Amendment Interests from Unreasonable Searches of Legally Seized Digital Data," *Houston Law Review* 51, no. 1 (n.d.): 153.

11 Athina Sachoulidou, "Cross-Border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift in the Area of 'Judicial' Cooperation,"

technologies complicate cybercrime governance, requiring stronger international collaboration and adaptable legal strategies to address new threats.[12] Accessing cross-border data stored in the cloud by law enforcement is fraught with legal and privacy issues, highlighting the need for clearer international agreements.[13]

Proposed cybercrime treaties risk expanding surveillance powers without adequate safeguards for privacy and due process, raising concerns about human rights.[14] Execution of mutual legal assistance requests in cybercrime cases is slow and inefficient, requiring streamlined mechanisms for cross-border cooperation.[15] Gaps in international frameworks hinder lawful access to electronic evidence, necessitating global solutions for accessing data across borders.[16] Jurisdictional challenges in U.S. cybercrime cases stem from the internet's global nature, often leading to enforcement difficulties and fragmented responses.[17]

Conflicts between territorial jurisdiction and global data flows require innovative solutions, such as shared governance models for data management.[18] Regional differences in policing strategies for cybercrime in Asia demonstrate the need for standardized approaches to tackle transnational cyber threats effectively.[19] Cross-border cybercrime investigations face delays due to language barriers, incompatible laws, and limited technical expertise among national agencies, suggesting the importance of capacity building and knowledge sharing. [20]

The reviewed literature offers significant strengths, including a robust analysis of jurisdictional and procedural challenges in cross-border cybercrime. However,

New Journal of European Criminal Law 15, no. 3 (September 6, 2024): 256–74, https://doi.org/10.1177/20322844241258649.

12 Evis Garunja et al., "Impact of Cyber Laws in Information Security Management to Protect Businesses and Citizens," in *Impact of Cyber Laws in Information Security Management to Protect Businesses and Citizens*, 2024, 617–28, https://doi.org/10.1007/978-981-97-6352-8_43.

13 Alexander J Pantos, "How the W How the World's Largest Economies Regulate Data Priv Conomies Regulate Data Privacy: Drawbacks, Benefits, & Proposed Solutions," *Indiana Journal of Global Legal Studie* 28, no. 2 (n.d.): 267–291.

14 Oxford Analytica, "Issue of State Control Impedes UN Treaty on Cybercrime," Emerald Expert Briefings, October 2, 2023, https://doi.org/10.1108/OXAN-DB282345.

15 Joshua I James and Pavel Gladyshev, "A Survey of Mutual Legal Assistance Involving Digital Evidence," *Digital Investigation* 18 (September 2016): 23–32, https://doi.org/10.1016/j.diin.2016.06.004.

16 Halefom H Abraha, "Regulating Law Enforcement Access to Electronic Evidence across Borders: The United States Approach," *Information & Communications Technology Law* 29, no. 3 (September 1, 2020): 324–53, https://doi.org/10.1080/13600834.2020.1794617.

17 Shuai Chen et al., "Exploring the Global Geography of Cybercrime and Its Driving Forces," *Humanities and Social Sciences Communications* 10, no. 1 (February 23, 2023): 71, https://doi.org/10.1057/s41599-023-01560-x.

18 Robert D Atkinson and Nigel Cory, "Cross-Border Data Policy: Opportunities and Challenges," 2021, 217–32, https://doi.org/10.1007/978-981-16-5391-9_20.

19 Azfer A Khan, "Reconceptualizing Policing for Cybercrime: Perspectives from Singapore," *Laws* 13, no. 4 (July 10, 2024): 44, https://doi.org/10.3390/laws13040044.

20 Fran Casino et al., "SoK: Cross-Border Criminal Investigations and Digital Evidence," *Journal of Cybersecurity* 8, no. 1 (January 28, 2022), https://doi.org/10.1093/cybsec/tyac014.

several weaknesses are evident. While the studies identify systemic issues, such as delays in mutual legal assistance and fragmented legal frameworks, they largely focus on theoretical solutions rather than actionable, empirical strategies. Moreover, most research addresses the challenges from a Western or regional perspective, leaving gaps in understanding the specific issues faced by developing countries or regions with limited cybercrime governance infrastructure.

A clear research gap emerges in the exploration of how artificial intelligence (AI) and machine learning can aid in cross-border cybercrime enforcement, an area with limited empirical data despite its growing relevance. Additionally, insufficient attention has been paid to developing a unified framework for balancing data sovereignty with international investigative needs. Future research could focus on creating adaptive legal protocols that leverage emerging technologies to streamline cross-border cooperation, particularly for underrepresented regions.

The objectives of this research are to analyze jurisdictional and procedural challenges in addressing cross-border cybercrimes. It evaluates the adequacy of existing international treaties and agreements on cybercrime. The study seeks to identify gaps in current international frameworks and practices. It focuses on enhancing cross-border cooperation in cybercrime investigations through improved procedures. The research also aims to develop adaptive legal frameworks for global effectiveness. It seeks to improve international cybercrime enforcement. The study emphasizes the importance of procedural efficiency in combating cybercrime globally. Its findings will contribute to stronger international collaboration in addressing cross-border cybercrime issues effectively.

The main research question of this research is: how can jurisdictional and procedural frameworks be adapted to address the challenges of cross-border cybercrime investigations while safeguarding privacy and due process?

The significance of this research lies in its growing challenges posed by cross-border cybercrime. As cybercrime knows no national boundaries, traditional legal frameworks are often inadequate to tackle transnational threats effectively. This research addresses coherent, flexible, and efficient jurisdictional and procedural frameworks for cross-border cybercrime investigations. The fragmentation of international legal instruments and the slow pace of mutual legal assistance hinder timely and effective responses to cybercriminal activities. Additionally, the rapid advancement of emerging technologies greatly aid in cybercrime investigations, remains underexplored in existing research. Moreover, the research will explore international cooperation with the protection of privacy rights, ensuring that due process safeguards are maintained despite the urgency of responding to cross-border cybercrime.

Methods

The research design for this study utilized a qualitative research methodology, applying a doctrinal research approach combined with comprehensive document analysis. This approach was specifically crafted to explore the intricate landscape of

cross-border e-crimes, with a particular focus on jurisdictional challenges and due process complexities. The study sought to provide a holistic understanding of the legal and procedural intricacies surrounding transnational cybercrime.

The target population for this research encompassed international regulations, policies, legal frameworks, and scholarly documents directly related to cybercrime jurisdiction. The sampling strategy was carefully designed to prioritize the most recent and relevant materials, with a specific emphasis on documents published after 2020 to ensure contemporary insights into the evolving landscape of digital crime and legal responses. This approach allowed for a comprehensive examination of the most current perspectives and challenges in the field.

Data collection was conducted through systematic searches across multiple academic and legal research platforms, including JSTOR, ProQuest, Web of Science, and Scopus. A meticulously developed keyword strategy was implemented to ensure thorough and targeted data retrieval. The research utilized an extensive list of keywords that captured the multifaceted nature of cross-border e-crimes, including terms such as cybercrime, transnational jurisdiction, digital forensics, extraterritoriality, mutual legal assistance, and electronic evidence, among others.

The primary research instruments consisted of academic databases and search platforms, supported by a structured analytical framework for document evaluation. To maintain the highest standards of research integrity, several rigorous measures were implemented. These included exclusive use of official legal documents from reputable sources, strict temporal delimitation, cross-referencing multiple sources to validate information, and ensuring transparent citation of all referenced materials.

The data analysis approach employed two primary techniques. Document analysis provided a systematic examination of scholarly articles, extracting thematic insights and legal interpretations. Simultaneously, the doctrinal research approach offered a comprehensive legal analysis of official documents, focusing on interpreting and synthesizing legal frameworks and their practical implications. This dual-method approach enabled a more nuanced and comprehensive understanding of the research topic.

Ethical considerations were paramount throughout the research process. The study exclusively utilized publicly available documents, maintained comprehensive and accurate referencing, and adhered to strict academic research integrity standards. The research acknowledges several inherent limitations that may impact the interpretation of findings. The rapidly evolving nature of cybercrime and digital law presents significant challenges to comprehensive analysis. Potential variations in international legal interpretations and the difficulty of generalizing findings across diverse jurisdictions were carefully considered. The study provides a general perspective on cross-border e-crimes, explicitly recognizing that legal landscapes are dynamic and subject to continuous transformation.

Results and Discussions

Cross-border cybercrime investigations face numerous complex challenges that significantly impede effective prosecution. The primary obstacles include the volatile nature of electronic evidence, which can be quickly deleted, transferred across jurisdictions, or encrypted, making preservation difficult.[21] Mutual legal assistance (MLA) requests are often slow and cumbersome, with execution hindered by conflicting national interests and coordination gaps. Jurisdictional conflicts are exacerbated by technological developments like cloud computing and anonymization tools, which obscure the physical location of perpetrators and criminal infrastructure. The rise of encryption, cryptocurrencies, and sophisticated organized criminal groups further complicate investigations, making it challenging to trace financial transactions and establish clear legal frameworks. Additionally, resource constraints, insufficient forensic expertise, and the lack of internationally agreed standards for electronic evidence collection create significant barriers.[22] The rapid proliferation of high-impact cyberattacks, combined with victims' reluctance to report incidents due to reputational concerns, compounds these investigative challenges.

The recent UN Cybercrime Treaty, allow states to exercise jurisdiction over cyber offenses based on the nationality of the victim or perpetrator, leading to fragmented enforcement. The "passive personality jurisdiction" can result in conflicting laws and enforcement actions that complicate international cooperation.[23] Each state may define cybercrimes differently, which undermines a unified approach to combating these offenses. For instance, the UN treaty extends its reach to any crime where evidence may be digital, raising concerns that it could lead to overreach and misuse. The drafting processes of many treaties have not adequately included perspectives from developing nations, which may face different challenges related to cybercrime.[24] Many agreements lack robust protections for privacy and freedom of expression. The volatile nature of digital evidence poses significant challenges for timely investigations across jurisdictions.

Emerging technologies are increasingly pivotal in enhancing cross-border cybercrime enforcement and investigations. AI-driven tools can analyze vast amounts of data quickly, identifying patterns and anomalies that would be difficult for human investigators to spot. For example, AI-powered systems can assist in

---

21 Casino et al.

22 Borka Jerman Blažič and Tomaž Klobučar, "Removing the Barriers in Cross-Border Crime Investigation by Gathering e-Evidence in an Interconnected Society," *Information & Communications Technology Law* 29, no. 1 (January 2, 2020): 66–81, https://doi.org/10.1080/13600834.2020.1705035.

23 Kenneth S Gallant, "The Passive Personality Principle," in *International Criminal Jurisdiction* (Oxford University PressNew York, 2022), 441–60, https://doi.org/10.1093/oso/9780199941476.003.0007.

24 Roman Girma Teshome, "The Draft Convention on the Right to Development: A New Dawn to the Recognition of the Right to Development as a Human Right?," *Human Rights Law Review* 22, no. 2 (March 4, 2022), https://doi.org/10.1093/hrlr/ngac001.

detecting fraudulent activities, financial crimes, and malware, accelerating investigation processes. Machine learning algorithms can enhance predictive analytics, improving threat detection and helping agencies anticipate future cybercriminal actions.[25] According to a 2023 report by the European Union Agency for Cybersecurity, AI-based tools have been shown to reduce investigation times by up to 40%, making them crucial for tackling transnational cybercrime efficiently. Furthermore, AI and ML can automate evidence gathering, helping law enforcement agencies overcome the delays and fragmentation that currently hinder international cooperation.[26]

The conflicting principles of data sovereignty and global investigative requires the development of unified legal frameworks that respect national rights while fostering international cooperation.[27] International instruments like the General Data Protection Regulation (GDPR) in the EU and the Cloud Act in the U.S. illustrate the tension between privacy protection and cross-border data access for law enforcement. The GDPR restricts data transfers outside the EU without adequate protecttion, complicating international investigations. In contrast, the Cloud Act mandates U.S. tech companies to provide data stored abroad upon request from U.S. law enforcement, potentially infringing on other countries' sovereignty. To address these tensions, frameworks such as the Budapest Convention on Cybercrime promote international cooperation but need further alignment to consider emerging data privacy standards. Unified frameworks could incorporate adaptable provisions that state sovereignty with necessary access for investigations, such as standardized protocols for mutual legal assistance, data encryption, and transparency measures for privacy protection.[28]

Developing countries face several significant challenges in cross-border cybercrime governance. They have limited budgets, resources, and governmental support for cybersecurity.[29] These nations often struggle with the slow implementation of international conventions such as the Budapest Convention on Cybercrime (2001), which aims to harmonize cybercrime laws and foster international cooperation. According to the United Nations Office on Drugs and Crime (UNODC), many

---

25 Stavros Kalogiannidis et al., "The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece," *Risks* 12, no. 2 (January 23, 2024): 19, https://doi.org/10.3390/risks12020019.

26 Luay Albtosh, "Automated Evidence Collection and Analysis Using AI," 2024, 143–86, https://doi.org/10.4018/979-8-3373-0588-2.ch006.

27 Mark Ryan, Paula Gürtler, and Artur Bogucki, "Will the Real Data Sovereign Please Stand up? An EU Policy Response to Sovereignty in Data Spaces," *International Journal of Law and Information Technology* 32, no. 1 (June 1, 2024), https://doi.org/10.1093/ijlit/eaae006.

28 Enver Buçaj and Kenan Idrizaj, "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention," *Multidisciplinary Reviews* 8, no. 1 (September 19, 2024): 2025024, https://doi.org/10.31893/multirev.2025024.

29 Chinazunwa Uwaoma and Ayush Enkhtaivan, "The Affordability of Cybersecurity Costs in Developing Countries: A Systematic Review," in *2024 IEEE International Conference on Cyber Security and Resilience (CSR)* (IEEE, 2024), 545–50, https://doi.org/10.1109/CSR61664.2024.10679506.

developing countries lack the necessary infrastructure and trained personnel to effectively combat cybercrime. Moreover, Different countries have different legal frameworks, definitions, and punishments for cybercrimes, which can lead to jurisdictional loopholes.[30] Strengthening partnerships through initiatives like the Global Forum on Cyber Expertise (GFCE) and promoting the African Union Convention on Cyber Security and Personal Data Protection (2014) can enhance cross-border cooperation and improve enforcement in these regions.

Jurisdictional and Procedural Frameworks Be Adapted to Safeguarding Privacy and Due Process

Traditional legal frameworks struggle with the borderless nature of cybercrime. Cybercriminals can operate seamlessly across multiple jurisdictions, making it difficult for national legal systems to investigate and prosecute crimes effectively. This issue is compounded by differing national laws regarding privacy protections, evidence collection, and data retention.[31] For example, the European Union's General Data Protection Regulation (GDPR) imposes strict rules on the collection and storage of personal data, while other countries may not have similar regulations, creating a patchwork of privacy protections across jurisdictions. The challenge becomes even more pressing as investigations require access to sensitive digital evidence, including personal data. Privacy concerns must be at the forefront, especially in light of increasing global data protection regulations like the Cross-Border Privacy Rules (Global CBPR frameworks 2023). Without careful regulation, digital investigations could inadvertently infringe upon citizens' rights to privacy.

A vital step towards addressing these challenges is the Budapest Convention on Cybercrime (2001), which lays the foundation for international cooperation in combating cybercrime. This treaty aims to standardize the definitions of cybercrimes, establish uniform procedures for electronic evidence collection, and streamline mutual legal assistance mechanisms. These efforts reduce the jurisdictional barriers that impede cross-border cybercrime investigations. By adhering to internationally accepted standards, countries can better navigate the complexities of digital offenses while ensuring that privacy and due process are respected. Further legal harmonization is necessary to create a unified, coherent framework for digital forensics and data-sharing protocols. International collaboration must be expanded, with countries committing to transparent, accountable procedures for obtaining and using evidence in cross-border investigations. This includes the development of uniform standards

[30] Yulia Razmetaeva, Hanna Ponomarova, and Iryna Bylya-Sabadash, "Jurisdictional Issues in the Digital Age," *Ius Humani. Law Journal* 10, no. 1 (April 12, 2021): 167–83, https://doi.org/10.31207/ih.v10i1.240.

[31] Dr Seema Singh and Prerna, "Regulation Of Cross-Border Data Flow And Its Privacy In The Digital Era," *NUJS Journal of Regulatory Studies* 9, no. 2 (May 30, 2024), https://doi.org/10.69953/njrs.v9i2.9.

for digital forensics, ensuring that investigative methods are consistent, reliable, and minimally intrusive.[32]

A multi collaborative approach is effective cybercrime investigations with safeguarding privacy and due process. National law enforcement agencies must work in tandem with international organizations such as Interpol and Europol to coordinate investigations. However, cooperation should extend beyond government agencies to include technology companies, civil society organizations, and academic institutions. Technology companies, for example, can provide expertise in securing encrypted data exchanges and developing AI-powered tools for threat detection, while civil society organizations can advocate for privacy protections and human rights. This model fosters a more comprehensive and balanced approach to cyber-crime investigations, where all stakeholders can contribute to developing solutions that are both effective and respectful of fundamental rights.[33]

Procedural safeguards must be incorporated into cybercrime investigations to protect privacy and due process. These safeguards include strict judicial oversight, where independent judges review digital investigations and approve warrants for accessing sensitive data. Privacy impact assessments should be mandatory for all digital investigations, ensuring that privacy concerns are addressed from the outset. Clear limitations on data collection and retention are necessary to prevent overreach, with transparency regarding the scope of digital evidence collection and retention processes. Furthermore, an independent oversight mechanism should be in place to ensure accountability and mitigate the risk of abuse of power. The legal and procedural frameworks should also include clear guidelines for data localization requirements, explicit consent for data collection, and the right to digital privacy.[34]

Advanced technological tools can support the adaptation of jurisdictional and procedural frameworks. For instance, secure, encrypted international evidence-sharing platforms can allow for safe cross-border data exchanges. AI-powered threat detection systems can help identify cybercrime patterns across borders, while machine learning algorithms can recognize suspicious activities that span multiple jurisdictions.[35] However, these technologies must be implemented with built-in privacy protections, ensuring that investigations do not infringe upon individuals' fundamental rights. Emerging legal principles such as proportionality in investigative

---

32 Naeem Allah Rakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations," *Mexican Law Review* 16, no. 2 (February 7, 2024): 23–54, https://doi.org/10.22201/iij.24485306e.2024.2.18892.

33 Nadia Gerspacher, "The Roles of International Police Cooperation Organizations," *European Journal of Crime, Criminal Law and Criminal Justice* 13, no. 3 (2005): 413–34, https://doi.org/10.1163/1571817054604100.

34 Radina Stoykova, "The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations," *Computer Law & Security Review* 49 (July 2023): 105801, https://doi.org/10.1016/j.clsr.2023.105801.

35 Mohammad Shahriar Rahman et al., "Accountable Cross-Border Data Sharing Using Blockchain Under Relaxed Trust Assumption," *IEEE Transactions on Engineering Management* 67, no. 4 (November 2020): 1476–86, https://doi.org/10.1109/TEM.2019.2960829.

measures and the right to digital privacy are critical to balancing law enforcement needs with privacy protections.

Primary limitations of existing international treaties and agreements

The rapid expansion of cybercrime presents significant challenges for existing international treaties and agreements, which were developed before the rise of sophisticated digital threats. One of the most significant limitations of international cybercrime treaties is the issue of jurisdiction. Cybercrime, by its nature, transcends national borders, making it difficult for any single nation to assert jurisdiction. This cross-border nature of cybercrime creates complex legal challenges, as cybercrimes may involve actors, victims, and data from multiple countries. As a result, existing international treaties often fail to provide clear and consistent jurisdictional rules for addressing cybercrimes.

The Budapest Convention, for instance, does not harmonize the definitions of cybercrime across different jurisdictions. Each country has its own legal framework, with varying standards for criminalizing digital offenses. Some countries have more extensive laws, while others may not criminalize certain acts, leading to challenges in prosecuting offenders. Additionally, differences in legal standards for evidence admissibility, such as the handling and transfer of digital evidence, make cross-border cooperation cumbersome.[36] Moreover, digital forensics techniques and investigative methods vary significantly, with some nations lacking the technological infrastructure to adequately collect and preserve evidence, complicating cooperation.

Another major limitation is the technological disparity between nations. The speed of technological advancements, especially in fields like artificial intelligence (AI), blockchain, and encryption, has far outpaced the development of international legal frameworks. Many international treaties were drafted before these technologies emerged, and as a result, they are ill-equipped to address the sophisticated nature of modern cyber threats. For instance, end-to-end encryption and decentralized systems such as blockchain complicate investigations and evidence collection.[37] While developed nations may have advanced technological capabilities and access to cutting-edge tools for digital forensics, developing countries often lack the resources and expertise necessary to investigate complex cybercrimes. This disparity exacerbates the challenges in establishing global cooperation, as nations with more advanced technological infrastructure may not be willing to share resources or support nations that are less capable in handling digital threats.

The Budapest Convention and other international agreements face significant enforcement challenges. While the convention sets out principles for cooperation, it

---

[36] Fernando Molina Granja and Glen D Rodríguez Rafael, "The Preservation of Digital Evidence and Its Admissibility in the Court," *International Journal of Electronic Security and Digital Forensics* 9, no. 1 (2017): 1, https://doi.org/10.1504/IJESDF.2017.081749.

[37] Hany F Atlam et al., "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions," *Electronics* 13, no. 17 (September 8, 2024): 3568, https://doi.org/10.3390/electronics13173568.

lacks robust enforcement mechanisms, leaving much of the implementation to the discretion of individual nations. This means that even though countries may agree to cooperate in principle, in practice, political tensions and differing national interests often hinder effective collaboration. For example, political tensions between countries, particularly those with divergent national security concerns, can impede the sharing of critical cyber intelligence. Furthermore, the lack of a comprehensive global mechanism for mandatory cybercrime cooperation means that many countries may not fully implement the treaty's provisions. Without standardized protocols for real-time response, cross-border information sharing, or mutual legal assistance, the international legal community struggles to mount a unified response to cybercrime.[38]

Another critical issue is the lack of consistency in legal procedures and protect-tions across jurisdictions. Different countries have varying definitions of cybercrime, making it difficult to create uniform international standards for prosecuting cyber-criminals. Moreover, the threshold for criminalizing digital offenses varies widely, with some countries only addressing certain types of cybercrime in their laws, while others have more expansive legal frameworks. Inconsistent data protection and privacy standards further complicate cooperation. Some nations have stringent privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union, while others may have less robust or conflicting privacy protect-tions. The challenges posed by these discrepancies are compounded by complex and time-consuming procedures for extradition, often making it difficult to bring cybercriminals to justice.[39]

Cybercrime's governance strategies

Cybercrime is a global threat that presents complex challenges, particularly for developing countries. One of the primary obstacles that developing countries face in addressing cybercrime is the lack of robust legal frameworks. Many nations still lack comprehensive laws to govern cybercrime, leaving gaps in their ability to effectively address digital threats. Legal reforms should start with aligning national laws with international standards, particularly with instruments like the Budapest Convention on Cybercrime.[40] This treaty sets standards for cooperation and establishes protocols for handling cybercrime, data privacy, and digital evidence across borders. The first step in this alignment process is Strategy Development. Countries need to under-stand the specific risks posed by cybercrime to their political, economic, and social systems. This understanding allows them to craft tailored strategies that align

[38] Noele Crossley, "Consistency, Protection, Responsibility," *Global Governance: A Review of Multilateralism and International Organizations* 26, no. 3 (September 17, 2020): 473–99, https://doi.org/10.1163/19426720-02603001.

[39] Michael Foran, "The Cornerstone Of Our Law: Equality, Consistency And Judicial Review," *The Cambridge Law Journal* 81, no. 2 (July 22, 2022): 249–72, https://doi.org/10.1017/S000819732200023X.

[40] Buçaj and Idrizaj, "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention."

cybercrime interventions with national objectives. In addition to this, national laws must clearly define cyber offenses, such as hacking, identity theft, and online fraud, ensuring that law enforcement agencies have the tools they need to investigate and prosecute crimes.

Building institutional capacity is another critical aspect of combating cybercrime. Developing countries often face a shortage of skilled professionals in cybersecurity, which weakens their ability to respond effectively to cyber threats. Governments must lay the groundwork by enacting appropriate laws, assigning operational mandates, and fostering collaboration between key stakeholders such as law enforcement, telecommunications companies, and financial institutions. This stage is key to ensuring that the necessary legislation and operational resources are in place to support cybercrime governance. Coordinating efforts ensures a more unified approach to tackling cybercrime, allowing resources and information to be shared efficiently across sectors.[41]

Technological infrastructure is another key challenge. Many developing countries struggle with outdated or inadequate cybersecurity infrastructure, which leaves them vulnerable to cyberattacks. Investing in national cybersecurity operations centers, advanced threat detection systems, and secure digital communication networks is essential. These investments will allow governments to detect and respond to cyber threats more effectively, minimizing the damage caused by cybercrime. Establishing Operational Capability emphasizes the importance of building technical capacity. Governments must equip their law enforcement and criminal justice systems with the tools and resources necessary for effective cybercrime investigations.[42] This includes developing specialized software for digital forensics, training staff to use advanced tools, and ensuring operational resources are sufficient for carrying out investigations.

International cooperation is vital when tackling cybercrime, as it is often a transnational issue. Cybercriminals frequently operate across borders, taking advantage of legal and jurisdictional gaps. Developing countries must engage in bilateral and multilateral agreements to facilitate the sharing of information and coordination of investigations. Tasking and Prioritization focuses on how governments can allocate resources efficiently and prioritize efforts based on the most pressing cyber threats. Strengthening international collaboration also involves establishing efficient information-sharing networks to ensure that threat intelligence can be quickly exchanged across borders, enabling a faster response to cyber

41 Alok Mishra et al., "Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations," *Computers & Security* 120 (September 2022): 102820, https://doi.org/10.1016/j.cose.2022.102820.

42 Carol A Archbold, "Police Accountability in the USA: Gaining Traction or Spinning Wheels?," *Policing: A Journal of Policy and Practice* 15, no. 3 (September 27, 2021): 1665–83, https://doi.org/10.1093/police/paab033.

incidents. Furthermore, fostering information-sharing protocols is essential for improving the speed and efficiency of responses to cyber incidents.[43]

A successful strategy for addressing cybercrime must include mechanisms for monitoring and evaluation. Governments should regularly assess the effectiveness of their cybercrime governance strategies and adjust them as necessary. This includes tracking the outcomes of individual investigations and evaluating the broader impact on public trust, national security, and economic stability. Regular feedback from law enforcement, the private sector, and civil society ensures that policies remain responsive to emerging threats. Governments should also implement metrics and reporting systems to track progress over time, enabling them to measure the success of their cybercrime efforts and identify areas for improvement.[44]

Conclusion

The digital age has ushered in an era of unprecedented opportunities and challenges, with cross-border e-crimes emerging as a significant threat to the global economy, national security, and individual privacy. As cybercrime becomes increasingly global, law enforcement must navigate complex legal boundaries, often encountering conflicting national laws and differing procedural norms. Emerging technologies like AI and machine learning, along with a unified legal approach, can improve cooperation between nations while protecting privacy and ensuring due process. The thesis of this research posits that current jurisdictional and procedural frameworks are insufficient for addressing the complexities of cross-border cybercrime. To enhance cross-border cooperation in cybercrime investigations, it is essential to adapt existing legal structures by integrating advanced technologies and creating new, flexible protocols where international investigative the protection of individual rights.

This study supports its thesis by analyzing the jurisdictional and procedural hurdles that hinder effective cross-border cybercrime enforcement. The role of emerging technologies, such as AI and machine learning, in improving international cooperation, particularly in underrepresented regions that often face challenges in cybercrime investigations. As cybercrime continues to evolve, it becomes increasingly clear that current legal structures are not adequately equipped to handle the complexities of cross-border enforcement. The opening statement identified the need for an updated approach, while the closing recommendation stresses the importance of leveraging emerging technologies and reforming international treaties to overcome jurisdictional challenges and protect due process in cybercrime investigations.

---

[43] Poopak Alaeifar et al., "Current Approaches and Future Directions for Cyber Threat Intelligence Sharing: A Survey," *Journal of Information Security and Applications* 83 (June 2024): 103786, https://doi.org/10.1016/j.jisa.2024.103786.

[44] Temitayo Oluwaseun Abrahams et al., "A Review Of Cybersecurity Strategies In Modern Organizations: Examining The Evolution And Effectiveness Of Cybersecurity Measures For Data Protection," *Computer Science & IT Research Journal* 5, no. 1 (January 9, 2024): 1–25, https://doi.org/10.51594/csitrj.v5i1.699.

An essential insight from this research is the realization that traditional legal frameworks are not designed for the rapidly changing technological landscape. While countries work within their own borders, cybercriminals exploit the lack of uniform international law enforcement, which calls for innovative solutions. Opponents may argue that increasing reliance on technology in cybercrime enforcement could compromise privacy and due process. However, this research argues that with the right safeguards, such as transparent oversight and clear legal boundaries, emerging technologies can enhance rather than hinder justice. Future research should focus on developing a unified, adaptive legal framework that incorporates emerging technologies like AI to address cross-border cybercrime effectively. This includes creating international treaties that consider the complexities of modern technology and data sovereignty, ensuring both global cooperation and the protection of individual rights. Further empirical studies are needed to assess the real-world application of these frameworks and their impact on cybercrime investigations.

References

Abraha, Halefom H. "Regulating Law Enforcement Access to Electronic Evidence across Borders: The United States Approach." *Information & Communications Technology Law* 29, no. 3 (September 1, 2020): 324–53. https://doi.org/10.1080/13600834.2020.1794617.

Alaeifar, Poopak, Shantanu Pal, Zahra Jadidi, Mukhtar Hussain, and Ernest Foo. "Current Approaches and Future Directions for Cyber Threat Intelligence Sharing: A Survey." *Journal of Information Security and Applications* 83 (June 2024): 103786. https://doi.org/10.1016/j.jisa.2024.103786.

Albtosh, Luay. "Automated Evidence Collection and Analysis Using AI," 143–86, 2024. https://doi.org/10.4018/979-8-3373-0588-2.ch006.

Allah Rakha, Naeem. "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations." *Mexican Law Review* 16, no. 2 (February 7, 2024): 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892.

Analytica, Oxford. "Issue of State Control Impedes UN Treaty on Cybercrime." Emerald Expert Briefings, October 2, 2023. https://doi.org/10.1108/OXAN-DB282345.

Archbold, Carol A. "Police Accountability in the USA: Gaining Traction or Spinning Wheels?" *Policing: A Journal of Policy and Practice* 15, no. 3 (September 27, 2021): 1665–83. https://doi.org/10.1093/police/paab033.

Atkinson, Robert D, and Nigel Cory. "Cross-Border Data Policy: Opportunities and Challenges," 217–32, 2021. https://doi.org/10.1007/978-981-16-5391-9_20.

Atlam, Hany F, Ndifon Ekuri, Muhammad Ajmal Azad, and Harjinder Singh Lallie. "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions." *Electronics* 13, no. 17 (September 8, 2024): 3568. https://doi.org/10.3390/electronics13173568.

Blažič, Borka Jerman, and Tomaž Klobučar. "Removing the Barriers in Cross-

Border Crime Investigation by Gathering e-Evidence in an Interconnected Society." *Information & Communications Technology Law* 29, no. 1 (January 2, 2020): 66–81. https://doi.org/10.1080/13600834.2020.1705035.

Buçaj, Enver, and Kenan Idrizaj. "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention." *Multidisciplinary Reviews* 8, no. 1 (September 19, 2024): 2025024. https://doi.org/10.31893/multirev.2025024.

Casino, Fran, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas, and Constantinos Patsakis. "SoK: Cross-Border Criminal Investigations and Digital Evidence." *Journal of Cybersecurity* 8, no. 1 (January 28, 2022). https://doi.org/10.1093/cybsec/tyac014.

Chambers, Frank. "An Ongoing Seizure: The Struggle to Uniformly Protect Fourth Amendment Interests from Unreasonable Searches of Legally Seized Digital Data." *Houston Law Review* 51, no. 1 (n.d.): 153.

Chen, Shuai, Mengmeng Hao, Fangyu Ding, Dong Jiang, Jiping Dong, Shize Zhang, Qiquan Guo, and Chundong Gao. "Exploring the Global Geography of Cybercrime and Its Driving Forces." *Humanities and Social Sciences Communications* 10, no. 1 (February 23, 2023): 71. https://doi.org/10.1057/s41599-023-01560-x.

Crossley, Noele. "Consistency, Protection, Responsibility." *Global Governance: A Review of Multilateralism and International Organizations* 26, no. 3 (September 17, 2020): 473–99. https://doi.org/10.1163/19426720-02603001.

Foran, Michael. "The Cornerstone Of Our Law: Equality, Consistency And Judicial Review." *The Cambridge Law Journal* 81, no. 2 (July 22, 2022): 249–72. https://doi.org/10.1017/S000819732200023X.

Gallant, Kenneth S. "The Passive Personality Principle." In *International Criminal Jurisdiction*, 441–60. Oxford University PressNew York, 2022. https://doi.org/10.1093/oso/9780199941476.003.0007.

Garunja, Evis, Akash Bag, Shouvik Kumar Guha, Neha Bharti, Mohit Tiwari, and Mohammed Salim Khan. "Impact of Cyber Laws in Information Security Management to Protect Businesses and Citizens." In *Impact of Cyber Laws in Information Security Management to Protect Businesses and Citizens*, 617–28, 2024. https://doi.org/10.1007/978-981-97-6352-8_43.

Gentile, Giulia. "Between Online and Offline Due Process: The Digital Services Act," 219–38, 2025. https://doi.org/10.1007/978-3-031-65381-0_11.

Gerspacher, Nadia. "The Roles of International Police Cooperation Organizations." *European Journal of Crime, Criminal Law and Criminal Justice* 13, no. 3 (2005): 413–34. https://doi.org/10.1163/1571817054604100.

Granja, Fernando Molina, and Glen D Rodríguez Rafael. "The Preservation of Digital Evidence and Its Admissibility in the Court." *International Journal of Electronic Security and Digital Forensics* 9, no. 1 (2017): 1. https://doi.org/10.1504/IJESDF.2017.081749.

James, Joshua I, and Pavel Gladyshev. "A Survey of Mutual Legal Assistance

Involving Digital Evidence." *Digital Investigation* 18 (September 2016): 23–32. https://doi.org/10.1016/j.diin.2016.06.004.

Kalogiannidis, Stavros, Dimitrios Kalfas, Olympia Papaevangelou, Grigoris Giannarakis, and Fotios Chatzitheodoridis. "The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece." *Risks* 12, no. 2 (January 23, 2024): 19. https://doi.org/10.3390/risks12020019.

Khan, Azfer A. "Reconceptualizing Policing for Cybercrime: Perspectives from Singapore." *Laws* 13, no. 4 (July 10, 2024): 44. https://doi.org/10.3390/laws13040044.

Klasén, Lena, Niclas Fock, and Robert Forchheimer. "The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age." *Forensic Science International* 362 (September 2024): 112133. https://doi.org/10.1016/j.forsciint.2024.112133.

Mishra, Alok, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, and Asif Qumer Gill. "Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations." *Computers & Security* 120 (September 2022): 102820. https://doi.org/10.1016/j.cose.2022.102820.

Moses Ashawa, Ali Mansour, Jackie Riley, Jude Osamor, and Nsikak Pius Owoh. "Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation." *Cloud Computing and Data Science* 5, no. 1 (December 25, 2023): 140–56. https://doi.org/10.37256/ccds.5120233845.

Onomrerhinor, F A Onomrerhinor. "Universal Jurisdiction For Transnational Cybercrimes?" *UCC Law Journal* 3, no. 1 (July 1, 2023): 119–51. https://doi.org/10.47963/ucclj.v3i1.1253.

Pantos, Alexander J. "How the W How the World's Largest Economies Regulate Data Priv Conomies Regulate Data Privacy: Drawbacks, Benefits, & Proposed Solutions." *Indiana Journal of Global Legal Studie* 28, no. 2 (n.d.): 267–291.

Razmetaeva, Yulia, Hanna Ponomarova, and Iryna Bylya-Sabadash. "Jurisdictional Issues in the Digital Age." *Ius Humani. Law Journal* 10, no. 1 (April 12, 2021): 167–83. https://doi.org/10.31207/ih.v10i1.240.

Ryan, Mark, Paula Gürtler, and Artur Bogucki. "Will the Real Data Sovereign Please Stand up? An EU Policy Response to Sovereignty in Data Spaces." *International Journal of Law and Information Technology* 32, no. 1 (June 1, 2024). https://doi.org/10.1093/ijlit/eaae006.

Sachoulidou, Athina. "Cross-Border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift in the Area of 'Judicial' Cooperation." *New Journal of European Criminal Law* 15, no. 3 (September 6, 2024): 256–74. https://doi.org/10.1177/20322844241258649.

Saeed, Saqib, Salha A Altamimi, Norah A Alkayyal, Ebtisam Alshehri, and Dina A Alabbad. "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations." *Sensors* 23, no. 15 (July 25, 2023): 6666. https://doi.org/10.3390/s23156666.

Shahriar Rahman, Mohammad, Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Guojon Wang. "Accountable Cross-Border Data Sharing Using Blockchain Under Relaxed Trust Assumption." *IEEE Transactions on Engineering Management* 67, no. 4 (November 2020): 1476–86. https://doi.org/10.1109/TEM.2019.2960829.

Singh, Dr Seema, and Prerna. "Regulation Of Cross-Border Data Flow And Its Privacy In The Digital Era." *NUJS Journal of Regulatory Studies* 9, no. 2 (May 30, 2024). https://doi.org/10.69953/njrs.v9i2.9.

Singh, Tripti. "Cybercrime And International Law: Jurisdictional Challenges And Enforcement Mechanisms." *African Journal of Biomedical Research*, September 23, 2024, 697–708. https://doi.org/10.53555/AJBR.v27i3S.2101.

Stoykova, Radina. "The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations." *Computer Law & Security Review* 49 (July 2023): 105801. https://doi.org/10.1016/j.clsr.2023.105801.

Temitayo Oluwaseun Abrahams, Sarah Kuzankah Ewuga, Samuel Onimisi Dawodu, Abimbola Oluwatoyin Adegbite, and Azeez Olanipekun Hassan. "A Review Of Cybersecurity Strategies In Modern Organizations: Examining The Evolution And Effectiveness Of Cybersecurity Measures For Data Protection." *Computer Science & IT Research Journal* 5, no. 1 (January 9, 2024): 1–25. https://doi.org/10.51594/csitrj.v5i1.699.

Teshome, Roman Girma. "The Draft Convention on the Right to Development: A New Dawn to the Recognition of the Right to Development as a Human Right?" *Human Rights Law Review* 22, no. 2 (March 4, 2022). https://doi.org/10.1093/hrlr/ngac001.

Uwaoma, Chinazunwa, and Ayush Enkhtaivan. "The Affordability of Cybersecurity Costs in Developing Countries: A Systematic Review." In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, 545–50. IEEE, 2024. https://doi.org/10.1109/CSR61664.2024.10679506.

Wicki-Birchler, David. "The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?" *International Cybersecurity Law Review* 1, no. 1–2 (October 22, 2020): 63–72. https://doi.org/10.1365/s43439-020-00012-5.

Zedner, Lucia, and Carl-Friedrich Stuckenberg. "Due Process." In *Criminal Justice and Procedure*, edited by Ambos Kai, Duff Antony, Roberts Julian, Weigend Thomas, and Heinze Alexander, I:304–342. Cambridge University Press, 2019.

Zubaidi, Fuad. "Territoriality in the Traditional Context." *Psychology and Behavioral Sciences* 2, no. 3 (2013): 89. https://doi.org/10.11648/j.pbs.20130203.12.