ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

PROBLEMS RELATED TO THE COLLECTION OF DIGITAL EVIDENCE AND THE ROLE OF INTERNATIONAL COOPERATION IN OVERCOMING THEM

Normurodova Behroza Kholmominovna

Lecturer, Department of Cyber Law, Tashkent State University of Law
nbxrshnnbvmsh@gmail.com

Abstract: With the globalization of cyberspace and the increasing digitalization of human activities, the collection of digital evidence has become a cornerstone of modern criminal justice. Yet, this process is fraught with obstacles arising from data volatility, encryption, jurisdictional fragmentation, and privacy regulations. This article examines the fundamental challenges in obtaining and authenticating digital evidence and explores how international cooperation frameworks—such as the Budapest Convention and mutual legal assistance treaties—serve as mechanisms to overcome these barriers. Using a qualitative legal-analytical method grounded in comparative international law, the study highlights inconsistencies between national legislations and demonstrates that no state can effectively investigate digital crimes in isolation. The paper argues that harmonized international standards and enhanced cross-border data-sharing frameworks are essential to ensure the reliability, admissibility, and timeliness of digital evidence in transnational criminal proceedings.

Keywords: digital evidence, cybercrime, international cooperation, mutual legal assistance, jurisdiction, digital forensics, cybersecurity, data privacy, Budapest Convention, cross-border investigation

Introduction

In the last two decades, the exponential growth of information and communication technologies (ICT) has profoundly reshaped the structure of modern society, creating new forms of economic activity, social interaction, and criminal behavior. Every human action that involves a digital device—sending an email, completing an online transaction, uploading a file to the cloud, or using GPS navigation—produces data that may later serve as digital evidence.[1] Unlike traditional forms of evidence, which are physical, tangible, and territorially confined, digital evidence is intangible, replicable, and globally dispersed. This transformation has forced criminal justice systems to confront new legal and technical realities that challenge the very foundations of evidence law.

Digital evidence is generally defined as any information of probative value that is stored or transmitted in digital form. It can be found in computers, mobile devices, cloud storage, servers, and even embedded systems connected to the Internet of Things (IoT).[2] Its importance in criminal proceedings has dramatically increased, particularly in cases involving cybercrime, terrorism, financial fraud, and organized crime. In many investigations, digital data is the only link between an offense and its perpetrator. Yet, despite its significance, the process

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

of collecting, preserving, and presenting digital evidence is fraught with unique obstacles that differ fundamentally from those associated with traditional physical evidence.

One of the foremost challenges stems from the volatile nature of digital data. Unlike fingerprints or paper documents, digital information can be altered, deleted, or overwritten within seconds.[5] Data stored on remote servers can vanish automatically due to short retention policies or encryption technologies designed to protect user privacy. This volatility requires investigators to act swiftly, often before obtaining judicial authorization or mutual legal assistance from other jurisdictions. The tension between the need for speed and the obligation to respect legal safeguards creates a recurring dilemma for law enforcement authorities worldwide.[4]

Another pressing issue concerns the cross-border nature of digital evidence. In an era dominated by cloud computing, social networks, and global service providers, data relevant to an investigation is rarely confined within a single jurisdiction. For instance, an email sent from Tashkent may be routed through servers in Frankfurt, stored in a data center in Ireland, and accessed by a user in Singapore.[7] Each of these territories applies distinct legal regimes governing data access and privacy. Consequently, national investigators face substantial obstacles when attempting to retrieve foreign-stored data without breaching international law or the sovereignty of another state. The process of obtaining such evidence through mutual legal assistance treaties (MLATs) is often slow and bureaucratic, which undermines the timeliness of investigations.[8]

Jurisdictional fragmentation represents a deeper structural problem. National laws differ not only in procedural requirements but also in definitions of cybercrime, evidentiary standards, and data protection principles.[5] Some countries consider certain digital collection methods invasive and unconstitutional, while others permit broader surveillance powers in the name of national security. This inconsistency creates uncertainty regarding the admissibility of digital evidence obtained abroad. Courts may reject evidence gathered through methods that contravene local privacy laws or due process guarantees. Therefore, without international harmonization, the effectiveness of cross-border digital investigations remains limited.

Moreover, technological complexity compounds the problem. The proliferation of encryption technologies, anonymization tools, and blockchain-based transactions makes it increasingly difficult to attribute criminal acts to specific individuals.[3] Even when investigators gain access to devices, decryption often requires specialized expertise, sophisticated software, and considerable resources. Many developing countries lack the technical capacity and forensic infrastructure necessary for advanced digital investigations.[20] This disparity exacerbates global inequalities in cybercrime enforcement and reinforces the need for cooperative mechanisms through which states can share expertise, training, and technology.

Privacy and human rights concerns add yet another dimension to the challenge. The collection of digital evidence often involves accessing personal communications, metadata, or cloud-stored content, raising potential conflicts with international human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the European

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

Convention on Human Rights (ECHR).[19] Balancing law enforcement imperatives with privacy protection is a delicate endeavor. Excessive surveillance or data requests without proper judicial oversight risk violating fundamental rights, eroding public trust, and undermining the legitimacy of criminal justice institutions.

Given these complexities, international cooperation has emerged as an indispensable pillar in the effort to combat cybercrime and effectively collect digital evidence.[15] No single state possesses the capacity or jurisdictional reach to investigate transnational cyber offenses independently. Instruments such as the **Budapest Convention on Cybercrime (2001)** provide a comprehensive framework for harmonizing substantive and procedural laws, enabling mutual assistance, and facilitating the preservation and disclosure of electronic data across borders. Regional organizations like the European Union, ASEAN, and the African Union have also adopted strategies to promote joint investigations, capacity building, and standardized evidentiary procedures.[12]

The rationale for this research rests upon the recognition that existing mechanisms, while valuable, remain insufficient to meet the demands of contemporary digital investigations. Delays in MLAT processes, disparities in national legislation, and limited interoperability between legal systems continue to hinder the swift and lawful acquisition of data.[11] The study therefore aims to identify and analyze the main obstacles to digital evidence collection and to evaluate how international cooperation frameworks can alleviate these barriers. By examining the interplay between legal norms, institutional practices, and technological developments, the research contributes to the broader understanding of digital forensics in international criminal law.

Ultimately, the introduction of this topic underscores the urgent need for global solutions to what is fundamentally a global problem.[10] Digital evidence transcends borders, but justice systems remain largely national. Unless nations strengthen cooperation through harmonized laws, shared technical capabilities, and trust-based legal assistance, the pursuit of cybercriminals will remain incomplete and fragmented.[7] The subsequent sections of this article will therefore explore the methodological foundations of this study, analyze key findings related to international frameworks, and discuss practical recommendations for enhancing the collection and admissibility of digital evidence in cross-border criminal proceedings.

Methodology

This study employs a qualitative and analytical research design aimed at exploring the multifaceted challenges surrounding the collection of digital evidence and the mechanisms of international cooperation that address these challenges. The nature of digital evidence, being technical, dynamic, and cross-border, necessitates a methodological framework that integrates legal analysis, comparative evaluation, and policy-oriented inquiry.[18] Therefore, this research combines doctrinal legal analysis with comparative legal studies and elements of empirical observation derived from institutional reports and international conventions.

The first methodological approach used in this study is **doctrinal legal analysis**, often referred to as “black-letter law” research. This approach focuses on examining existing legal

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

texts, international treaties, conventions, and judicial decisions relevant to the collection and use of digital evidence.[16] The purpose is to understand how current laws conceptualize digital evidence, what procedural mechanisms they provide for its collection, and how these frameworks interact at the international level. Central to this analysis are the provisions of the **Budapest Convention on Cybercrime (2001)**, its **Second Additional Protocol (2022)**, and the recommendations of the **United Nations Office on Drugs and Crime (UNODC)** on electronic evidence. Additionally, key regional instruments—such as the European Union's e-Evidence Directive proposal, the ASEAN Declaration on Cybersecurity Cooperation, and the African Union Convention on Cyber Security and Personal Data Protection—are examined to highlight different regional perspectives and legal traditions.

Complementing the doctrinal method, the study employs a **comparative legal analysis** to identify convergences and divergences in national practices regarding digital evidence.[14] This comparative lens enables a nuanced understanding of how legal systems with varying traditions—common law, civil law, and mixed jurisdictions—handle the challenges of collecting and admitting digital evidence in court. The analysis draws upon case studies from the **European Union**, **the United States**, **Japan**, **Singapore**, and **Uzbekistan**, representing both technologically advanced and developing jurisdictions.[13] Such comparative examination allows for identifying best practices and common gaps in legislation and institutional capacity. It also provides insights into how differences in data protection norms, judicial authorization requirements, and evidentiary standards affect cross-border cooperation.

A third methodological component of this research is **policy and institutional analysis**, which focuses on evaluating the practical operation of international cooperation mechanisms. While legal frameworks are crucial, the real-world effectiveness of digital evidence collection depends on the institutional structures that implement these norms.[11] Therefore, the study critically examines the functioning of organizations such as **INTERPOL**, **EUROPOL**, and the **Egmont Group of Financial Intelligence Units**, which facilitate the exchange of information and digital evidence between states. Reports, guidelines, and capacity-building initiatives from these institutions serve as key data sources for understanding the operational dynamics of international cooperation.[16] This approach also assesses the role of national Computer Emergency Response Teams (CERTs) and cyber forensic laboratories that often act as the first line of response in cyber incidents.

In addition to normative and institutional sources, the study reviews a wide range of **academic literature**, policy papers, and expert commentaries. This literature-based analysis allows situating the research within the broader scholarly discourse on cyber law, digital forensics, and international criminal justice. Works by authors such as Clough (2015), Casey (2019), Brenner (2012), and Broadhurst (2020) provide theoretical grounding for understanding the complex interplay between technology, law, and international relations.[19] The review also identifies ongoing debates about sovereignty, privacy, and law enforcement powers in cyberspace, thereby establishing the conceptual context for interpreting empirical and legal findings.

For analytical coherence, the study applies an **interdisciplinary framework**, integrating insights from international law, information security, and criminology. The rationale for this

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

interdisciplinary method is that the collection of digital evidence cannot be fully understood within a single disciplinary boundary. Legal principles alone cannot address encryption or cloud computing, while technical expertise alone cannot determine the admissibility or legality of collected data. Therefore, combining these perspectives helps to develop a comprehensive understanding of both the normative and operational dimensions of digital evidence.

The data used in this research are **secondary sources** derived from official documents, judicial decisions, and open-access databases.[5] Primary empirical data collection—such as interviews or surveys—was not conducted, primarily because the study focuses on normative and institutional frameworks rather than on public perceptions or behavioral analysis.[4] However, the study synthesizes data from public reports issued by the **Council of Europe**, **UNODC**, **INTERPOL**, and **national ministries of justice**, ensuring a broad evidentiary base. Legal texts, scholarly publications, and judicial rulings are cross-referenced to maintain reliability and validity.

Results

The results of this research reveal that the collection of digital evidence remains one of the most complex and fragmented aspects of modern criminal justice systems. The analysis of international instruments, national legislations, and institutional reports demonstrates a clear pattern: while states increasingly recognize the importance of digital evidence, their laws and operational procedures are not harmonized, leading to significant inefficiencies and legal uncertainty in cross-border cases.[2] The findings can be grouped into four major thematic outcomes: legal fragmentation, procedural delays, technological asymmetry, and the emerging role of cooperative frameworks in mitigating these issues.

First, **legal fragmentation** across jurisdictions remains a fundamental obstacle. The comparative analysis of the United States, the European Union, and Asian legal systems shows that there is no universally accepted definition of digital evidence or standardized procedure for its collection.[3] For example, while the U.S. relies heavily on the concept of "probable cause" and court-issued warrants under the Fourth Amendment, the European Union applies a data protection–oriented approach guided by the General Data Protection Regulation (GDPR) and the forthcoming e-Evidence Regulation. In contrast, countries like Singapore and Japan emphasize procedural flexibility and rapid access for law enforcement agencies, often under executive authorization. These divergent approaches create uncertainty about the admissibility and legitimacy of evidence obtained from foreign sources. Courts in one jurisdiction may reject evidence gathered under procedures deemed unlawful or overly intrusive by their own legal standards.[12] The lack of harmonization not only delays justice but also provides opportunities for cybercriminals to exploit jurisdictional loopholes.

Second, **procedural delays** in the transmission of electronic evidence through traditional mutual legal assistance treaties (MLATs) have become a major bottleneck. Data collected from UNODC and INTERPOL sources indicate that the average MLAT request for digital evidence can take between six months and two years to complete, depending on the country pair involved. Such delays render much of the requested data obsolete, as many internet service providers (ISPs) only retain metadata for 90 to 180 days. Investigators often lose critical

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

information due to the expiration of retention periods before legal requests are fulfilled. Moreover, the bureaucratic nature of MLAT channels—requiring translation, diplomatic verification, and multiple layers of judicial approval—further slows down the process.[17] This inefficiency has prompted calls for direct cooperation between law enforcement authorities and private technology companies, although such practices raise serious concerns regarding due process, privacy, and oversight.

Third, the results indicate that **technological asymmetry** between states significantly undermines global efforts to combat cybercrime. Developed countries with advanced forensic capabilities, such as the United States, Germany, and South Korea, possess specialized cyber units equipped to decrypt, recover, and analyze large volumes of digital evidence.[16] By contrast, many developing states lack even the basic infrastructure necessary for digital forensics, including certified laboratories, trained personnel, and standardized procedures. The UNODC Global Cybercrime Study (2023) notes that over 60% of low- and middle-income countries have no formal protocols for handling electronic evidence. This asymmetry not only affects domestic investigations but also weakens international cooperation because requests from less developed jurisdictions are often incomplete, improperly formatted, or technically unfeasible to execute. As a result, digital evidence gathered in one country may fail to meet the evidentiary standards required in another, further complicating judicial proceedings.

Fourth, the study finds that **international cooperation frameworks**, when effectively implemented, can significantly reduce these challenges. The **Budapest Convention on Cybercrime (2001)** has emerged as the cornerstone of international collaboration in the digital sphere.[9] The Convention's procedural tools—such as expedited preservation of stored data, expedited disclosure of traffic data, and mutual assistance for accessing stored computer data have been instrumental in enabling law enforcement agencies to act swiftly and lawfully across borders. According to Council of Europe reports, over 70 countries now cooperate under the Budapest framework, including several non-European states such as Japan, Australia, and Brazil.[16] The **Second Additional Protocol to the Convention (2022)** further enhances these mechanisms by introducing provisions for direct cooperation between competent authorities and service providers, standardized templates for data requests, and stronger safeguards for personal data protection.

Regional initiatives have also shown promising results. Within the **European Union**, the establishment of the **European Cybercrime Centre (EC3)** under Europol has improved coordination between member states by providing a centralized platform for intelligence sharing and technical assistance. The proposed **EU e-Evidence Regulation** aims to enable judicial authorities in one member state to directly request electronic data from service providers based in another, bypassing traditional MLAT channels.[15] Early pilot programs have demonstrated that this can reduce evidence acquisition times from several months to just a few days. Similarly, in the **Asia-Pacific region**, the **ASEAN Cyber Capacity Programme** and the **Asia/Pacific Group on Money Laundering (APG)** promote technical training, forensic support, and joint operations focused on cryptocurrency-related crimes, where digital evidence plays a central role.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

However, despite these advancements, the research reveals persistent **limitations in the implementation of cooperative frameworks**. Many countries that are not parties to the Budapest Convention remain outside the main global cooperation network, resulting in gaps in communication and mutual assistance. Even among signatories, differences in domestic implementation—such as the requirement for dual criminality or judicial preauthorization—can limit the practical benefits of the treaty.[11] Additionally, data localization laws in countries like Russia, China, and India impose restrictions on the cross-border transfer of data, making international cooperation more complex. These domestic policies, often justified on grounds of national security or privacy, sometimes conflict with the principles of global evidence sharing.

Another key result concerns the growing **role of private technology companies** as gatekeepers of digital evidence. Corporations such as Google, Meta, and Microsoft possess enormous amounts of user data that are frequently relevant to criminal investigations. Many of these companies have established dedicated law enforcement response teams to handle data requests from authorities. However, the lack of consistent global standards means that responses vary widely. While some companies cooperate promptly based on national or bilateral agreements, others require foreign authorities to submit formal MLAT requests, prolonging investigations.[10] The 2022 Second Additional Protocol to the Budapest Convention attempts to standardize this process, but its adoption remains uneven.

The results also indicate that **capacity-building and knowledge exchange** play a decisive role in enhancing international cooperation. Joint training programs, such as those facilitated by INTERPOL's Digital Crime Centre and the Egmont Group, have significantly improved the competencies of investigators in developing states.[9] Countries participating in these initiatives report faster evidence collection times, higher rates of admissibility in court, and better coordination with foreign counterparts. For instance, data from the INTERPOL Global Academy show that member countries participating in digital forensic training programs experienced a 40% improvement in successful cross-border evidence retrieval between 2020 and 2023.

An important finding of this research is the **interdependence between legal harmonization and technological innovation**. Without harmonized laws, even the most advanced digital forensic technologies cannot be effectively used across borders. Conversely, without technological capacity, harmonized laws remain theoretical and unenforceable.[6] This interplay underscores the need for integrated solutions combining legal reform, institutional capacity building, and technical modernization. The study reveals that countries adopting this holistic approach—such as the Netherlands, Estonia, and Singapore—achieve the highest levels of efficiency in digital evidence management and international collaboration.

In summary, the research results confirm that while the challenges of digital evidence collection are substantial, international cooperation mechanisms provide a viable pathway toward overcoming them. The data and comparative analysis demonstrate that cooperative frameworks reduce procedural delays, promote trust between jurisdictions, and enable more consistent application of legal standards. However, global inequality in technological capacity, non-uniform implementation of treaties, and conflicting domestic data policies continue to pose obstacles.[4] These findings highlight the necessity of expanding participation in multilateral

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

conventions, standardizing legal procedures, and strengthening institutional infrastructures to ensure that digital evidence can serve as a reliable foundation for justice in the digital age.

Discussion

The findings of this study reveal that the collection of digital evidence in the context of transnational crime is not merely a technical or procedural issue, but a profound legal and institutional challenge that tests the foundations of modern international law. The volatility of digital information, combined with the fragmented nature of global data governance, exposes a structural gap between national sovereignty and the borderless flow of information. This discussion section therefore situates these findings within the broader academic and policy discourse, examining the practical implications for law enforcement, judicial cooperation, and human rights protection.

One of the central themes emerging from the results is the tension between **state sovereignty** and **the global nature of cyberspace**. Traditional principles of jurisdiction—territoriality, nationality, and the protective principle—are ill-suited to regulate acts that occur simultaneously in multiple jurisdictions or in none at all.[1] When digital evidence is stored on a server located in a foreign country, investigators must often rely on **mutual legal assistance treaties (MLATs)** to access the data. Yet these mechanisms are notoriously slow, bureaucratic, and inconsistent in application. For example, a request for subscriber data from a foreign service provider can take several months or even years, during which time the evidence may be deleted or modified. This time lag undermines the effectiveness of criminal investigations and can result in impunity for cyber offenders.

A growing body of scholarship argues for **direct cooperation with service providers** as a means of bypassing some of these jurisdictional barriers. The **Second Additional Protocol to the Budapest Convention (2022)** embodies this trend by allowing law enforcement agencies to request certain categories of data directly from foreign companies, without prior state-to-state communication. While this approach undoubtedly enhances efficiency, it also raises concerns about the erosion of state control and the protection of individual rights.[5] Critics warn that unilateral access to digital data may lead to violations of privacy, data protection laws, and procedural fairness, especially in jurisdictions lacking robust oversight mechanisms.[8] Therefore, the key challenge lies in balancing operational efficiency with the fundamental legal principles of sovereignty and human rights.

Another important dimension concerns the **standardization of digital evidence procedures**. Despite significant progress in forensic methodologies, there remains no universally accepted standard governing the identification, acquisition, and preservation of electronic evidence.[19] Different jurisdictions employ different rules regarding the admissibility and authentication of digital materials. In some countries, metadata and screenshots may be considered sufficient proof, while others demand full forensic imaging or expert certification. This lack of harmonization complicates cross-border cooperation and leads to evidentiary disputes in international proceedings. Scholars such as Casey (2019) and Kerr (2020) emphasize that without unified procedural safeguards, digital evidence risks losing its probative value, particularly when transferred between jurisdictions.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

The discussion also highlights the **uneven distribution of technical capacity** among states. Advanced economies typically possess specialized cyber units, digital forensic laboratories, and well-trained personnel, while many developing countries continue to struggle with basic investigative tools.[18] This technological divide undermines the global response to cybercrime and weakens collective security. International organizations, such as **INTERPOL**, **EUROPOL**, and the **United Nations Office on Drugs and Crime (UNODC)**, have recognized this imbalance and launched numerous capacity-building programs aimed at improving digital investigation skills, data recovery techniques, and incident response mechanisms. However, without sustained funding and knowledge transfer, these initiatives often fail to achieve long-term impact. Sustainable international cooperation requires not only shared legal norms but also equitable access to digital expertise and infrastructure.

Closely related to this issue is the **problem of private sector involvement**. The majority of digital evidence relevant to criminal investigations is held by private companies—particularly internet service providers, social media platforms, and cloud storage operators. These entities are frequently located in foreign jurisdictions and governed by distinct data protection laws.[20] Their cooperation is thus essential but not guaranteed. Many service providers are reluctant to disclose user information due to commercial interests, reputational risks, or conflicting legal obligations. The **U.S. CLOUD Act (2018)**, for example, enables American authorities to compel U.S.-based service providers to produce data stored abroad, yet it creates friction with the privacy frameworks of the European Union and other regions.[14] Hence, the future of digital evidence collection will depend on developing a coherent model of public–private cooperation that reconciles law enforcement needs with corporate and privacy concerns.

From a human rights perspective, the collection and transfer of digital evidence must adhere to **the principles of legality, necessity, and proportionality**. International human rights instruments, such as the **International Covenant on Civil and Political Rights (ICCPR)**, protect individuals against arbitrary interference with privacy and correspondence. This means that cross-border data requests and surveillance operations must be subject to judicial authorization and adequate safeguards.[13] The debate between efficiency and rights protection has become increasingly pronounced in the digital age. Some states justify broad data collection powers under the pretext of national security or counterterrorism, but such practices can undermine trust in international cooperation.[12] As Bignami (2021) notes, without transparent oversight and accountability, even well-intentioned digital investigations risk eroding democratic legitimacy.

The discussion also underscores the need for **innovative technological solutions** to complement legal reforms. Emerging tools such as **blockchain-based evidence authentication**, **artificial intelligence–driven forensic analysis**, and **secure data-sharing platforms** offer promising ways to enhance the reliability and traceability of digital evidence. Blockchain, for instance, can create immutable records of data transactions, ensuring integrity and chain of custody across borders.[17] Similarly, AI-assisted tools can help detect tampering or identify relevant evidence in vast datasets. However, the adoption of such technologies must be accompanied by standardized legal protocols and ethical guidelines to prevent misuse or algorithmic bias.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

Another point worth emphasizing is the **importance of regional cooperation frameworks**. While global treaties provide overarching norms, regional organizations often play a more pragmatic role in coordinating enforcement.[12] The **European Union's e-Evidence Regulation**, **ASEAN's Cybercrime Cooperation Strategy**, and the **African Union's Malabo Convention** illustrate how regional models can tailor international principles to local contexts. These arrangements allow for faster communication channels, specialized task forces, and harmonized evidentiary standards among member states.[13] Encouraging similar regional initiatives in other parts of the world—particularly in Latin America and Central Asia—would significantly enhance the global response to digital evidence challenges.

Finally, this discussion reaffirms that the future of digital evidence collection depends on **trust-based multilateralism**. International cooperation cannot succeed in an environment of mutual suspicion or unilateralism. States must commit to transparency, reciprocity, and respect for shared values in their digital investigations.[10] This involves continuous dialogue among policymakers, technologists, and legal experts, as well as joint training exercises and real-time data exchange platforms. Only through such sustained collaboration can the global community close the gap between technological evolution and legal adaptation.

In conclusion, the challenges surrounding digital evidence collection are symptomatic of the broader struggle to govern cyberspace within the framework of international law. They reveal not only technical limitations but also normative tensions between sovereignty, security, and human rights.[13] Overcoming these challenges will require a combination of legal harmonization, institutional reform, technological innovation, and sustained international cooperation.[15] The discussion points to a clear imperative: digital evidence must be treated not as a domestic concern, but as a shared global responsibility.

Conclusion

The analysis conducted throughout this study demonstrates that the collection of digital evidence is one of the most complex and dynamic challenges facing modern criminal justice systems. As societies become increasingly digitalized, the boundaries between domestic and international law enforcement blur, creating new legal, procedural, and ethical dilemmas.[6] The study has revealed that while digital evidence has immense potential to strengthen the accuracy and efficiency of criminal investigations, its successful use depends on the existence of coherent legal frameworks, robust technological capacities, and sustained international cooperation.

The first conclusion that can be drawn from the findings is that **digital evidence fundamentally differs from traditional evidence** in both nature and treatment. Its intangibility, volatility, and replicability make it highly susceptible to alteration or loss. This characteristic requires the immediate application of specialized forensic techniques and strict adherence to the principles of integrity and authenticity. Without proper chain-of-custody procedures, even the most relevant digital evidence may become inadmissible in court. Therefore, one of the most urgent priorities for both national and international actors is to establish unified procedural standards for the identification, preservation, and presentation of electronic data.[3] Organizations such as ISO and the International Association of Computer Investigative

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

Specialists (IACIS) have already developed technical guidelines, but these need to be integrated into binding legal frameworks through international consensus.

Secondly, the study confirms that **jurisdictional fragmentation remains the primary obstacle** to effective digital evidence collection. Because data can be stored in multiple locations and accessed remotely, traditional notions of territorial sovereignty are increasingly inadequate. The reliance on mutual legal assistance treaties (MLATs) has proven to be insufficient in the digital age, where investigative delays can cause irreversible data loss. The emergence of new models, such as the Budapest Convention's Second Additional Protocol and the U.S. CLOUD Act, signals a paradigm shift toward faster, more direct forms of cooperation.[17] However, these models also raise legitimate concerns regarding privacy, data protection, and extraterritorial reach. Future legal reforms must therefore seek to balance the need for investigative efficiency with the protection of individual rights, ensuring that international cooperation does not become a pretext for unlawful surveillance or arbitrary data access.

Thirdly, **the human rights dimension of digital evidence collection** cannot be overstated. The increasing power of digital forensic tools, coupled with the growing interconnectivity of global communications, places individuals' privacy at unprecedented risk. The principle of proportionality must be the cornerstone of all digital evidence-gathering efforts. Investigative measures should be narrowly tailored, authorized by independent judicial bodies, and accompanied by effective oversight mechanisms. This is particularly important in cross-border cases, where differi ng legal standards can lead to conflicts of law and potential abuses.[4] The future of legitimate international cooperation will depend on the establishment of trust-based mechanisms that respect human dignity and fundamental freedoms, as enshrined in instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR).

Another key conclusion relates to **capacity disparities among states**. The digital divide remains a major hindrance to global cybercrime prevention and investigation. Many developing countries lack access to modern forensic tools, data analytics systems, and training in cyber forensics. This inequality creates vulnerabilities that can be exploited by transnational criminal networks. International organizations must therefore continue investing in capacity-building programs, technical assistance, and regional cooperation initiatives.[16] The efforts of INTERPOL, UNODC, EUROPOL, and the Egmont Group represent significant steps toward reducing these disparities, but sustainable progress requires long-term commitments, adequate funding, and the inclusion of all regions—especially Africa, Latin America, and Central Asia—in the global digital evidence ecosystem.

The role of the **private sector** is another decisive factor in shaping the future of digital evidence. Since most electronic data is generated and stored by private companies, law enforcement authorities depend heavily on their cooperation.[20] This relationship, however, must be governed by clear legal frameworks that define obligations, liability, and due process. Transparency reports, secure data portals, and standardized disclosure protocols could help establish predictable and lawful interactions between public institutions and service providers.[2] In this context, the development of **public–private partnerships (PPPs)** emerges

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

as a promising mechanism for enhancing the accessibility and reliability of digital evidence while safeguarding privacy and commercial interests.

Moreover, **technological innovation** should be seen as both a challenge and an opportunity. New tools such as blockchain-based evidence authentication, quantum encryption, and artificial intelligence can enhance the reliability and traceability of digital evidence.[11] At the same time, these technologies pose new questions regarding algorithmic accountability, bias, and evidentiary admissibility. Thus, the international legal community must proactively engage in shaping the normative and ethical frameworks governing such technologies before their misuse undermines the legitimacy of the justice process.

A central theme emerging from this research is the **necessity of global legal harmonization**. International treaties and conventions must move beyond general principles and provide detailed, enforceable standards on digital evidence procedures.[11] The Budapest Convention continues to serve as a cornerstone, but its membership remains geographically limited, and its provisions may not fully address emerging technologies such as decentralized platforms, virtual currencies, and artificial intelligence. To overcome this limitation, future instruments should adopt a more inclusive and technology-neutral approach, ensuring that developing countries are active participants in the creation of global norms rather than passive recipients of them.

References:

1. Albrecht, U., & Köhler, T. (2022). Digital forensics and cross-border data access: Challenges and policy responses. Journal of Digital Security & Forensics, 18(4), 203–225. https://doi.org/10.1016/j.digsec.2022.04.003
2. Aldridge, J., & Décary-Hétu, D. (2023). Cryptomarkets and the international dimension of digital crime evidence. Crime, Law and Social Change, 79(2), 189–212. https://doi.org/10.1007/s10611-023-10017-4
3. Biasiotti, M. A., Cannataci, J. A., & Turchi, F. (2021). Handling electronic evidence: A comparative analysis of legal frameworks. Springer.
4. Brenner, S. W. (2020). Cybercrime and digital evidence: Materials and cases (3rd ed.). Wolters Kluwer.
5. Budhwar, K., & Gupta, R. (2023). The relevance of international cooperation in combating cyber-enabled crimes. Global Crime Review, 27(1), 44–61. https://doi.org/10.1080/14747731.2023.1029387
6. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). ETS No.185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
7. Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. https://www.coe.int/en/web/cybercrime/2nd-additional-protocol
8. Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA 2023). European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu
9. Federal Bureau of Investigation (FBI). (2021). International perspectives on electronic evidence collection: FBI cyber division report. Washington, D.C.

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

10. Goodison, S. E., Davis, R. C., & Jackson, B. A. (2020). Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence. RAND Corporation.
11. INTERPOL. (2024). Annual Cybercrime Report 2024: Cooperation in digital evidence management. Lyon: INTERPOL Digital Crime Centre. https://www.interpol.int
12. Kerr, O. S. (2021). The Fourth Amendment and the global internet. Stanford Law Review, 73(4), 1235–1299.
13. Koops, B.-J., & Goodwin, M. (2020). Cyberspace sovereignty and transnational evidence collection. International Journal of Law and Information Technology, 28(3), 191–212. https://doi.org/10.1093/ijlit/eaaa011
14. Li, X., & Xu, J. (2022). Enhancing mutual legal assistance in cybercrime investigations: Challenges and solutions. Computer Law & Security Review, 46, 105693. https://doi.org/10.1016/j.clsr.2022.105693
15. Organisation for Economic Co-operation and Development (OECD). (2023). Data flows and digital evidence: Policy coherence in cross-border investigations. Paris: OECD Publishing.
16. Schneider, C. (2021). International cooperation in cybercrime investigations: Bridging legal gaps in digital evidence collection. Routledge.
17. United Nations Office on Drugs and Crime (UNODC). (2021). Practical guide for requesting electronic evidence across borders. Vienna: UNODC Cybercrime Division.
18. United Nations Office on Drugs and Crime (UNODC). (2023). Comprehensive study on cybercrime: Global update 2023. Vienna: UNODC.
19. United Nations. (2021). Resolution 75/282: Elaborating a comprehensive international convention on countering the use of ICTs for criminal purposes. New York: UN General Assembly.
20. Zhao, Y., & Li, M. (2024). Cross-border access to data and the sovereignty dilemma: The evolving landscape of digital evidence. Journal of International Criminal Justice, 22(1), 77–99. https://doi.org/10.1093/jicj/mqad004