INTERNATIONAL JOURNAL OF LAW AND SOCIAIL SCIENCES
Vol. 2, No. 2, June 2026
https://ijlss.net/

Legal Challenges of Digital Evidence in Criminal Proceedings: Comparative Perspectives from Pakistan, Indonesia, and Malaysia

Anwar Ali
Muslim Youth University, Islamabad, Pakistan
bll232012@myu.edu.pk

Maryam Bilal
Chenab Law Collage, Gujrat, Pakistan
maryambilal7866@gmail.com

Sarmad Malik
Muslim Youth University, Islamabad, Pakistan
bll232023@myu.edu.pk

ABSTRACT

The rapid digitalization of modern societies has transformed criminal investigations and judicial proceedings, leading to an unprecedented reliance on digital evidence in the administration of justice. Electronic communications, social media content, mobile device data, cloud storage records, surveillance footage, blockchain transactions, and digital forensic reports have become increasingly important in the detection, prosecution, and adjudication of criminal offenses. Despite these developments, significant legal and procedural challenges remain regarding the admissibility, authenticity, reliability, and evaluation of digital evidence in criminal proceedings. This study examines the legal challenges associated with digital evidence through a comparative analysis of Pakistan, Indonesia, and Malaysia, three Muslim-majority jurisdictions that have undertaken substantial legislative reforms in response to technological advancements and cyber-related crimes.Employing a qualitative doctrinal and comparative legal methodology, the research analyzes constitutional provisions, criminal procedure laws, cybercrime legislation, electronic transaction regulations, judicial decisions, and international standards governing digital evidence. The study explores key issues relating to the authentication and integrity of electronic evidence, chain of custody requirements, digital forgery and manipulation, cybersecurity vulnerabilities, privacy and data protection concerns, and cross-border evidentiary challenges arising from transnational digital communications. The comparative analysis demonstrates that while Pakistan, Indonesia, and Malaysia have established legal frameworks recognizing the evidentiary value of digital materials, significant differences remain regarding admissibility standards, forensic capabilities, judicial interpretation, and institutional capacity.The findings reveal that the increasing sophistication of digital technologies presents challenges that traditional evidentiary rules are often ill-equipped to address. Inconsistent legal standards, limited forensic resources,

jurisdictional complexities, and the growing prevalence of artificial intelligence-generated content further complicate the effective use of digital evidence in criminal trials. The study argues that greater legal harmonization, enhanced forensic infrastructure, specialized judicial training, and stronger regional cooperation are necessary to ensure the reliability and fairness of digital evidence in criminal justice systems. It concludes by proposing a harmonized framework for digital evidence governance that balances technological innovation, procedural fairness, and the protection of fundamental rights within contemporary criminal proceedings.

Keywords: Digital Evidence; Criminal Proceedings; Electronic Evidence; Cybercrime Law; Digital Forensics.

INTRODUCTION

The rapid advancement of digital technologies has fundamentally transformed contemporary societies, economies, and legal systems. Over the past two decades, the widespread adoption of smartphones, cloud computing, artificial intelligence, social media platforms, blockchain technologies, and internet-based communication systems has generated unprecedented volumes of electronic data. As human interactions increasingly occur within digital environments, criminal activities have also evolved, utilizing sophisticated technological tools that transcend geographical boundaries and challenge traditional law enforcement mechanisms. Consequently, criminal justice systems worldwide are experiencing a paradigm shift in the manner in which evidence is collected, preserved, authenticated, and presented before courts. In this evolving landscape, digital evidence has emerged as one of the most significant components of modern criminal investigations.[1]

Digitalization has not only changed the methods through which crimes are committed but has also transformed the nature of evidence used to establish criminal liability. Traditionally, criminal proceedings relied heavily upon physical evidence, eyewitness testimony, documentary records, and confessions. However, contemporary investigations frequently involve electronic communications, emails, mobile phone records, social media interactions, GPS data, surveillance footage, digital financial transactions, cloud storage records, and metadata generated through various digital devices. Such forms of evidence often provide critical insights into criminal behavior, enabling investigators to

[1] Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs*, *3*(5). https://doi.org/10.71317/rjsa.003.05.0375

reconstruct events with a degree of precision previously unattainable through conventional investigative methods.[2]

The growing significance of digital evidence has become particularly evident in cases involving cybercrime, terrorism financing, online fraud, money laundering, human trafficking, corruption, narcotics offenses, and transnational organized crime. Criminal actors increasingly exploit digital technologies to conceal their identities, transfer illicit funds, communicate securely, and coordinate unlawful activities across multiple jurisdictions. As a result, prosecutors and law enforcement agencies now depend extensively upon digital evidence to establish factual connections between suspects and criminal conduct. In many instances, digital evidence serves as the primary or even sole source of proof available to investigators.[3]

The increasing reliance upon digital evidence has generated substantial legal and procedural challenges within criminal justice systems. Unlike traditional forms of evidence, digital information can be easily altered, manipulated, duplicated, deleted, or fabricated without leaving visible traces. The authenticity and integrity of electronic records therefore become central concerns during criminal proceedings. Courts must determine whether digital evidence has been lawfully obtained, properly preserved, and accurately presented. Questions regarding chain of custody, forensic reliability, admissibility standards, and technological expertise frequently arise, requiring judges and legal practitioners to navigate complex intersections between law and technology.[4]

Recent technological developments have further intensified these challenges. The emergence of artificial intelligence has facilitated the creation of highly sophisticated deepfakes capable of manipulating audio, video, and image content with remarkable realism. Such technologies raise serious concerns regarding evidentiary reliability and the potential misuse of fabricated digital materials in criminal investigations. Similarly, encrypted communication platforms, decentralized networks, virtual private networks (VPNs), and blockchain-based transactions have complicated efforts to identify perpetrators and collect admissible evidence. These developments highlight the urgent need

---

[2] Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. In *Proceedings - 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)* (pp. 11–20). IEEE. https://doi.org/10.1109/tps-isa62245.2024.00012

[3] Romaniuk, V., & Ablamskyi, S. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law and Safety*, (2), 143–152. https://doi.org/10.32631/pb.2024.2.13

[4] Petryk, V. V. (2025). Vykorystannia elektronnykh dokaziv u kryminalnomu provadzhenni: problemy yikh zboru, perevirky ta otsinky [The use of electronic evidence in criminal proceedings: issues of collection, verification, and evaluation]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo* [*Uzhhorod National University Herald. Series: Law*], *87*(4), 119–123. https://doi.org/10.24144/2307-3322.2025.87.4.17

for legal systems to adapt their evidentiary frameworks to contemporary technological realities.[5]

The legal regulation of digital evidence varies considerably across jurisdictions. While many countries have enacted legislation governing electronic transactions, cybercrime, and digital investigations, significant differences remain regarding admissibility requirements, evidentiary standards, forensic procedures, and judicial interpretation. These variations become particularly important in cross-border criminal investigations where digital evidence may originate from multiple jurisdictions simultaneously. The absence of harmonized standards often creates legal uncertainty, delays criminal proceedings, and undermines international cooperation in combating transnational crime.[6]

Within the context of Muslim-majority countries, Pakistan, Indonesia, and Malaysia provide particularly valuable case studies for examining the legal challenges associated with digital evidence. These jurisdictions have experienced rapid digital transformation and substantial growth in internet penetration, electronic commerce, digital financial services, and online communication. Simultaneously, they have undertaken significant legal reforms to address cybercrime and regulate electronic evidence within criminal proceedings. Despite these developments, questions remain regarding the effectiveness of existing legal frameworks in addressing emerging technological challenges.[7]

Pakistan has introduced several legislative measures governing electronic evidence, including cybercrime regulations and provisions relating to digital investigations. However, practical challenges persist concerning forensic capacity, evidentiary authentication, judicial expertise, and procedural consistency. Similarly, Indonesia has developed an extensive legal framework regulating electronic information and transactions, yet courts continue to confront difficulties related to evidentiary reliability, privacy protection, and technological complexity. Malaysia, often regarded as one of the region's most technologically advanced legal systems, has established comprehensive legislation concerning digital evidence, but ongoing developments in artificial

[5] Shyshenko, A. O. (2025). Tsyfrovye dokazy u kryminalnomu provadzhenni: problemy avtentychnosti ta dopustymosti [Digital evidences in criminal proceedings: problems of authenticity and admissibility]. *Analitychno-Porivnialne Pravoznavstvo* [*Analytical and Comparative Jurisprudence*], *5*(3), 312–316. https://doi.org/10.24144/2788-6018.2025.05.3.46

[6] Matis, J. (2024). Certain aspects of criminal evidence and digital evidence. *Analytical and Comparative Jurisprudence*, (2), 701–705. https://doi.org/10.24144/2788-6018.2024.02.116

[7] Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, *16*(2), 23–44. https://doi.org/10.22201/iij.24485306e.2024.2.18892

intelligence, cybersecurity, and cross-border investigations continue to generate novel legal questions.[8]

The comparative examination of these three jurisdictions is particularly timely given the increasing interconnectedness of criminal activities in Southeast Asia and South Asia. Cybercriminal networks frequently operate across national borders, exploiting differences in legal systems and enforcement capacities. Consequently, understanding how Pakistan, Indonesia, and Malaysia regulate digital evidence can provide valuable insights into broader regional efforts aimed at strengthening criminal justice systems and enhancing international legal cooperation.

Despite the growing body of scholarship on digital evidence, significant gaps remain in the comparative legal literature. Existing studies often focus on individual jurisdictions or specific categories of cybercrime without systematically analyzing the broader legal challenges associated with digital evidence in criminal proceedings. Furthermore, recent technological developments, particularly artificial intelligence, cloud computing, and encrypted communications, have introduced new evidentiary concerns that remain insufficiently addressed within many legal frameworks. There is therefore a pressing need for comparative research that critically evaluates the strengths and weaknesses of existing approaches while proposing practical solutions for future reform.[9]

Against this background, the central research problem addressed in this study concerns the inadequacy of existing legal and procedural frameworks in effectively regulating the collection, authentication, admissibility, and evaluation of digital evidence within criminal proceedings. While Pakistan, Indonesia, and Malaysia have adopted legislative measures recognizing electronic evidence, significant challenges continue to undermine its effective utilization in practice. These challenges include inconsistencies in evidentiary standards, limitations in forensic infrastructure, concerns regarding privacy and due process rights, difficulties in maintaining chain of custody, and the increasing sophistication of technologies capable of manipulating digital information.

To address this problem, the study seeks to answer the following research questions:

---

[8] Luhina, N., & Paliukh, O. (2025). Peculiarities of proof in criminal proceedings related to cybercrime. *Social Development: Economic and Legal Issues*, (4), 205–214. https://doi.org/10.70651/3083-6018/2025.4.27

[9] Didenko, O. V. (2025). Tsyfrova kryminalistyka ta mizhnarodna protydiia kiberzlochynnosti (na prykladi elektronnoi komertsii) [Digital forensics and international counteraction to cybercrime (based on the example of e-commerce)]. *Analitychno-Porivnialne Pravoznavstvo* [*Analytical and Comparative Jurisprudence*], *4*(3), 162–167. https://doi.org/10.24144/2788-6018.2025.04.3.26

1. What legal frameworks govern the admissibility and evaluation of digital evidence in criminal proceedings in Pakistan, Indonesia, and Malaysia?
2. What are the principal legal, procedural, and technological challenges affecting the use of digital evidence within these jurisdictions?
3. How do judicial institutions in Pakistan, Indonesia, and Malaysia address issues relating to authenticity, reliability, integrity, and chain of custody of digital evidence?
4. What comparative lessons can be derived from the experiences of these jurisdictions to strengthen digital evidence regulation and criminal justice effectiveness?
5. How can a more harmonized and technologically responsive legal framework be developed to address emerging challenges associated with digital evidence in the digital age?

The primary objective of this study is to critically examine the legal challenges surrounding the use of digital evidence in criminal proceedings through a comparative analysis of Pakistan, Indonesia, and Malaysia. Specifically, the study aims to evaluate existing legislative frameworks, identify practical and procedural obstacles, assess judicial approaches toward electronic evidence, and develop recommendations for legal reform. Through comparative analysis, the research seeks to contribute to the development of more effective evidentiary standards capable of responding to contemporary technological realities.

The significance of this research extends beyond the jurisdictions under examination. Academically, the study contributes to emerging scholarship at the intersection of criminal law, evidence law, cyber law, and digital governance. It provides a contemporary comparative perspective that enhances understanding of how legal systems adapt to technological transformation. Practically, the findings may assist policymakers, legislators, judges, prosecutors, and law enforcement agencies in developing more robust legal frameworks for managing digital evidence. At the international level, the research offers insights into harmonization efforts aimed at strengthening cross-border cooperation against cybercrime and other technology-facilitated offenses.

As digital technologies continue to reshape criminal behavior and investigative practices, the effective regulation of digital evidence will remain a defining challenge for modern criminal justice systems. The ability of legal institutions to balance technological innovation, evidentiary reliability, procedural fairness, and fundamental rights will play a crucial role in determining the effectiveness and legitimacy of criminal proceedings in the twenty-first

century. Through a comparative examination of Pakistan, Indonesia, and Malaysia, this study seeks to advance scholarly understanding and contribute to the ongoing development of responsive and future-oriented legal frameworks for digital evidence.

Methodology and Scope

This study adopts a qualitative doctrinal and comparative legal research methodology to examine the legal challenges associated with the use of digital evidence in criminal proceedings. The research primarily relies on the analysis of primary legal sources, including constitutions, criminal procedure laws, electronic transaction statutes, cybercrime legislation, judicial decisions, and relevant regulations governing digital evidence in Pakistan, Indonesia, and Malaysia. Secondary sources such as academic journal articles, books, policy reports, international guidelines, and legal commentaries are also utilized to provide theoretical and contextual support.

The comparative approach enables a systematic evaluation of similarities and differences among the legal frameworks of the selected jurisdictions. Pakistan, Indonesia, and Malaysia were chosen due to their significant digital transformation, evolving cybercrime legislation, and growing reliance on electronic evidence within criminal justice systems. The study further examines how courts and law enforcement authorities address key evidentiary issues, including authenticity, integrity, admissibility, chain of custody, forensic reliability, and privacy protection. The research is limited to criminal proceedings involving digital evidence and does not extensively analyze civil or commercial litigation. Particular attention is given to contemporary challenges arising from technological developments such as artificial intelligence, deepfake technologies, encrypted communications, cloud computing, social media platforms, and cross-border cybercrime investigations. The study also considers relevant international standards and best practices relating to electronic evidence management and digital forensic procedures.

By focusing on these three jurisdictions, the research seeks to identify common challenges, evaluate the effectiveness of existing regulatory mechanisms, and propose recommendations for legal reform and regional harmonization. Ultimately, the study aims to contribute to the development of a more coherent and technologically responsive framework for the collection, authentication, admission, and evaluation of digital evidence in modern criminal justice systems.

Theoretical and Legal Foundations of Digital Evidence

Theoretical and legal foundations of digital evidence have become central to contemporary criminal justice systems as social, commercial, and governmental

activities increasingly occur through digital technologies. The proliferation of smartphones, cloud computing, social media platforms, artificial intelligence, blockchain systems, and Internet-of-Things (IoT) devices has transformed both the commission of crimes and the methods used to investigate them. Unlike traditional evidence, digital evidence is intangible, easily replicable, highly volatile, and often distributed across multiple jurisdictions. These characteristics require a distinct legal and theoretical framework capable of addressing issues of authenticity, integrity, reliability, privacy, and cross-border cooperation.[10]

Concept and Definition of Digital Evidence

Digital evidence generally refers to information of probative value that is stored, transmitted, or generated in digital form and can be used to establish facts in legal proceedings. International forensic literature commonly defines digital evidence as information and data of investigative value that is stored on, received, or transmitted by electronic devices. This broad definition encompasses not only the visible content of digital communications but also the metadata associated with those communications, such as timestamps, geolocation records, device identifiers, and network logs.Contemporary legal systems increasingly recognize digital evidence as equivalent in principle to documentary or physical evidence, provided that its authenticity and integrity can be established. However, digital evidence differs from traditional evidence in several important respects. First, it is often highly volatile; data can be modified, overwritten, or deleted within seconds. Second, it is infinitely replicable, meaning identical copies may exist simultaneously in multiple locations. Third, it is frequently dependent on technological systems for interpretation, requiring specialized forensic expertise. Finally, digital evidence is commonly embedded within complex technical environments such as cloud infrastructures, encrypted platforms, and distributed networks. These characteristics have significant legal implications. Courts must determine whether electronic records accurately represent the events they purport to document, whether the data has been altered, and whether the methods used to collect and preserve the evidence satisfy procedural fairness. Consequently, the concept of digital evidence is inseparable from questions of forensic methodology and legal reliability.[11]

---

[10] Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs*, *3*(5). https://doi.org/10.71317/rjsa.003.05.0375

[11] Asgarova, M. P., Aliyev, B. A. O., Khalilov, F. Y., & Hasanova, I. Z. K. (2022). The use of electronic evidence in court: A comparative legal analysis in the world practice. *Cuestiones Políticas*, *40*(72), 373–388. https://doi.org/10.46398/cuestpol.4072.21

Types of Digital Evidence in Contemporary Criminal Investigations

Digital evidence encompasses a broad range of electronically stored or transmitted information that can be used to establish facts relevant to criminal investigations and judicial proceedings. One major category is device-based evidence, which includes data recovered from computers, smartphones, tablets, external storage devices, and wearable technologies, such as documents, photographs, videos, browsing histories, application data, and even deleted files. Another important category consists of network and communication records, including Internet Protocol (IP) logs, email headers, call detail records, messaging-platform metadata, and network traffic captures that help investigators reconstruct communications and online activities. Increasingly significant is cloud-stored data, which comprises information maintained on remote servers, such as cloud backups, synchronized files, online accounts, and collaborative digital workspaces; however, the transnational nature of cloud storage frequently raises complex issues of jurisdiction, privacy, and cross-border access. Social media evidence has also emerged as a critical source of information, encompassing posts, comments, private messages, live-stream content, and user interaction records from platforms such as Facebook, Instagram, TikTok, WhatsApp, and X, which are frequently utilized in investigations involving fraud, harassment, extremism, terrorism, and organized crime. Financial and transactional data constitute another vital category, including electronic banking records, mobile payment transactions, cryptocurrency wallet activity, and blockchain transaction histories that play a crucial role in uncovering money laundering, corruption, financial crimes, and cyber fraud. Additionally, the rapid expansion of the Internet of Things (IoT) has introduced new forms of evidence generated by smart devices, connected vehicles, surveillance systems, and digital sensors capable of providing location, movement, environmental, and behavioral data relevant to criminal investigations. Given the diversity, complexity, and continuous evolution of these sources, modern legal systems must develop flexible and technologically adaptive evidentiary frameworks capable of ensuring the admissibility, authenticity, and reliability of digital evidence while safeguarding fundamental rights and procedural fairness.[12]

Principles of Admissibility, Authenticity, and Chain of Custody in Digital Evidence

The admissibility of digital evidence in criminal proceedings depends upon several fundamental evidentiary principles that are widely recognized across legal systems. First, digital evidence must be relevant, meaning that it must have a

[12] Osco Escobedo, M. A., Chipana Fernández, Y. M. M., Quiñones Li, A. E., Díaz-Pérez, J. J., Calvo de Oliveira Diaz, D. G., & Garcia Quispe, G. B. (2023). Digital evidence as a means of proof in criminal proceedings. *Russian Law Journal*, *11*(5s). https://doi.org/10.52783/rlj.v11i5s.895

logical connection to a fact in issue and assist the court in resolving a material question. Second, authenticity requires proof that the electronic record is genuinely what it purports to be, which may be established through forensic examination, metadata analysis, witness testimony, system logs, and cryptographic verification methods. Closely related is the principle of integrity, which demands that the evidence remain complete and unaltered from the time of acquisition until its presentation in court. To preserve integrity, investigators commonly employ forensic imaging, write-blocking technologies, secure storage procedures, and cryptographic hash functions. Reliability constitutes another essential requirement, as courts increasingly scrutinize whether the methods, forensic tools, and expert analyses used to collect and interpret digital evidence are scientifically sound and generally accepted within the digital forensics community. Furthermore, the legality of acquisition remains a critical consideration, since evidence obtained through unlawful searches, unauthorized interception, or violations of privacy and due process rights may be excluded from judicial proceedings. These principles have gained heightened significance in the age of artificial intelligence and deepfake technologies, where AI-generated audio, video, and images can convincingly imitate real individuals, thereby necessitating advanced forensic authentication techniques before such evidence can be considered trustworthy. Equally important is the maintenance of an unbroken chain of custody, which refers to the documented process governing the collection, handling, transfer, storage, examination, and presentation of digital evidence. Effective chain-of-custody management requires the identification of the evidence source, the use of validated forensic acquisition procedures such as bit-by-bit imaging, the generation and verification of cryptographic hash values, detailed documentation of all transfers between responsible personnel, secure physical and digital storage, and comprehensive audit trails capable of independent review. Because digital information can be easily copied, modified, or corrupted, any failure in chain-of-custody procedures may compromise the authenticity, integrity, and evidentiary value of the material, potentially leading courts to question its reliability or exclude it altogether. Consequently, robust admissibility standards and rigorous chain-of-custody protocols remain indispensable for ensuring the credibility and legal acceptance of digital evidence in contemporary criminal justice systems.[13]

International Standards, Evidentiary Theories, and Contemporary Challenges of Digital Evidence

[13] Ahmadian, M. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, *11*(1), Article 19. https://doi.org/10.1186/s41935-021-00234-6

The globalization of cybercrime and digital communications has significantly increased the importance of international standards in regulating the collection, preservation, and admissibility of electronic evidence. Key frameworks such as the Council of Europe Budapest Convention on Cybercrime, ISO/IEC 27037 standards, NIST Digital Forensics Guidelines, and operational protocols developed by INTERPOL Interpol and regional organizations provide guidance on digital evidence preservation, forensic integrity, cross-border cooperation, and investigative best practices. These frameworks emphasize forensic repeatability, tool validation, comprehensive documentation, privacy protection, and growing concerns regarding AI-generated evidence. Theoretical approaches to digital evidence continue to evolve, encompassing real evidence theory, which views digital traces such as surveillance recordings and server logs as direct representations of events; documentary evidence theory, which treats electronic records as legally valid documents; hearsay and reliability theory, which examines the evidentiary status of automated system-generated records; and the best evidence principle, which adapts traditional concepts of originality to digital environments where identical copies can coexist. Furthermore, modern investigations increasingly employ probabilistic and data-driven approaches that rely on metadata analysis, network correlations, large datasets, and AI-assisted forensic tools. The emergence of artificial intelligence presents both opportunities and risks, as AI can generate or analyze evidence while simultaneously raising concerns regarding bias, opacity, explainability, and fabrication. Contemporary legal debates focus primarily on deepfakes and synthetic media that challenge traditional authentication methods, encryption technologies that create tensions between privacy rights and lawful access to evidence, and cross-border data access issues arising from cloud computing and jurisdictional complexities. Consequently, the legal and theoretical foundations of digital evidence are undergoing continuous transformation, requiring legal systems to integrate traditional evidentiary principles with technologically informed procedures that ensure evidential reliability while safeguarding privacy, due process, and fundamental human rights in the digital age.[14]

REGULATORY FRAMEWORK GOVERNING DIGITAL EVIDENCE IN PAKISTAN, INDONESIA, AND MALAYSIA

The increasing reliance on digital technologies in communication, commerce, governance, and criminal activity has compelled legal systems worldwide to modernize their evidentiary frameworks. Digital evidence has become indispensable in the investigation and prosecution of cybercrime, financial fraud, terrorism, corruption, money laundering, online harassment, and transnational organized crime. Consequently, Pakistan, Indonesia, and Malaysia have enacted legislative measures to recognize electronic records, regulate cyber

[14] Rashkovsk, D., & Rashkovska, V. (2025). The difference between digital evidence and evidence in digital form. *Iustinianus Primus Law Review*, *16*(2), 68–79. https://doi.org/10.55302/iplr2516268r

activities, and establish procedures for the collection and admissibility of digital evidence. Despite these developments, significant differences remain regarding evidentiary standards, investigative powers, privacy protections, and judicial approaches to electronic evidence.

Pakistan's Legal Framework

Pakistan's legal framework governing digital evidence is primarily shaped by the Prevention of Electronic Crimes Act (PECA) 2016, the Qanun-e-Shahadat Order 1984, the Electronic Transactions Ordinance (ETO) 2002, and relevant provisions of criminal procedure legislation. The Electronic Transactions Ordinance represented Pakistan's first major effort to provide legal recognition to electronic documents, electronic signatures, and digital communications. The Ordinance established the principle that electronic records should not be denied legal effect solely because they exist in digital form. The Prevention of Electronic Crimes Act 2016 significantly expanded Pakistan's regulatory approach by criminalizing unauthorized access, cyberterrorism, electronic fraud, identity theft, data interference, and other technology-related offenses. PECA also grants investigative authorities powers to obtain electronic evidence, preserve data, conduct searches, and seize digital devices subject to legal safeguards. The Qanun-e-Shahadat Order has been interpreted to permit the admissibility of electronic evidence, including digital documents, surveillance recordings, and electronic communications, provided that authenticity and reliability can be demonstrated. However, practical challenges remain concerning forensic capacity, evidentiary authentication, chain-of-custody management, and judicial expertise in handling technologically complex cases. Recent developments have highlighted additional concerns regarding digital privacy, government surveillance, encrypted communications, and cross-border data access. As cybercrime continues to evolve, legal scholars increasingly argue that Pakistan's evidentiary framework requires modernization to address emerging technologies such as artificial intelligence, deepfake content, blockchain transactions, and cloud-based data storage.[15]

Indonesia's Legal Framework

Indonesia has developed one of Southeast Asia's most comprehensive legal frameworks governing electronic information and digital evidence. The primary legislation is the Electronic Information and Transactions Law (ITE Law), initially enacted in 2008 and subsequently amended to address evolving

[15] Zahoor, R., Waqar Khan Arif, S. M., & Bannian, B. (2022). Digital evidence and its admissibility under Pakistani law. *Journal of Development and Social Sciences*, *3*(4), 51–60. https://doi.org/10.47205/jdss.2022(3-iv)06

technological challenges. The ITE Law recognizes electronic information and electronic documents as valid legal evidence and establishes rules governing electronic transactions, digital communications, and cyber-related offenses. Under Indonesian law, electronic information, digital documents, emails, electronic contracts, and computer-generated records may serve as admissible evidence in judicial proceedings. The legal framework recognizes electronic evidence as an extension of traditional evidentiary categories while maintaining requirements relating to authenticity, integrity, and reliability. Indonesia has also enacted legislation addressing cybercrime, personal data protection, and digital governance. These reforms reflect growing concerns regarding cybersecurity threats, online fraud, misinformation, hate speech, and unauthorized access to computer systems. In criminal proceedings, investigators are empowered to obtain electronic evidence through lawful investigative measures, including digital forensic examinations and data preservation orders.

However, the rapid growth of digital platforms and cloud-based technologies has generated new legal challenges. Courts increasingly confront disputes involving social media evidence, encrypted communications, cryptocurrency transactions, and cross-border digital investigations. The emergence of artificial intelligence-generated content has further complicated evidentiary assessments, particularly regarding authenticity and manipulation. Consequently, Indonesia continues to refine its regulatory framework to balance effective law enforcement with constitutional protections relating to privacy, freedom of expression, and due process.[16]

Malaysia's Legal Framework

Malaysia is widely regarded as one of the region's pioneers in digital law and electronic evidence regulation. The country has established a relatively sophisticated legal framework through legislation such as the Evidence Act 1950, the Computer Crimes Act 1997, the Digital Signature Act 1997, the Communications and Multimedia Act 1998, and the Electronic Commerce Act 2006. A particularly significant development was the incorporation of provisions within the Evidence Act that explicitly recognize computer-generated documents and electronic records as admissible evidence. Malaysian courts have developed extensive jurisprudence addressing issues of digital authentication, forensic reliability, electronic communications, and evidentiary integrity. This judicial experience has contributed to greater certainty regarding the treatment of digital evidence in criminal proceedings. The Computer Crimes Act criminalizes unauthorized access, modification, and misuse of computer systems, while the Communications and Multimedia Act regulates online communications and digital networks. Together, these laws provide a

[16] Dhumillah, D. S. R. (2024). The stand of electronic evidence in cyber crime law enforcement in Indonesia. *Eduvest - Journal of Universal Studies*, *4*(9), 4215–4226. https://doi.org/10.59188/eduvest.v4i9.1812

comprehensive framework for investigating technology-related offenses and obtaining electronic evidence. Malaysia's legal system has also demonstrated increasing engagement with contemporary technological developments, including cybersecurity threats, digital financial services, cryptocurrency activities, and artificial intelligence applications. Nevertheless, challenges remain concerning encrypted communications, transnational cybercrime investigations, and the evidentiary implications of rapidly evolving technologies. Like many jurisdictions, Malaysia faces the ongoing task of ensuring that legal standards remain responsive to technological innovation without undermining fundamental rights and procedural fairness.[17]

Electronic Transaction and Cybercrime Laws

Across Pakistan, Indonesia, and Malaysia, electronic transaction legislation serves as the foundation for recognizing the legal validity of digital records. These laws generally establish that electronic documents, electronic signatures, and digital communications possess legal force equivalent to their traditional paper-based counterparts. Such recognition is essential because criminal investigations increasingly rely on electronically stored information generated through routine social and economic activities. In addition to electronic transaction laws, all three jurisdictions have enacted cybercrime legislation addressing offenses such as unauthorized access, data interference, cyber fraud, identity theft, online harassment, and cyberterrorism. These statutes typically provide investigative authorities with powers to preserve digital data, access computer systems pursuant to legal authorization, and collect electronic evidence for criminal proceedings. However, legislative responses to emerging technologies vary. Questions surrounding cryptocurrency transactions, artificial intelligence-generated content, cloud storage, and encrypted messaging platforms continue to challenge traditional legal concepts. The increasing use of cross-border digital services further complicates enforcement efforts because evidence frequently resides outside national jurisdictions. Consequently, cybercrime laws increasingly require mechanisms for international cooperation and mutual legal assistance.[18]

Criminal Procedure Provisions Relating to Digital Evidence

[17] D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The chain of custody in the era of modern forensics: From the classic procedures for gathering evidence to the new challenges related to digital data. *Healthcare*, *11*(5), Article 634. https://doi.org/10.3390/healthcare11050634

[18] Hasanah, L. N., Faisal, M. S., Ahmed, Z., & Hasyim, M. Y. A. (2025). Religious diversity and the digital economy: Legal–academic pathways to harmonize Sharia and international law. *International Journal of Law and Social Sciences*, *1*(1). https://doi.org/10.65960/ijlss.1.1.2025.8

The admissibility and use of digital evidence depend not only upon substantive legislation but also upon procedural safeguards governing criminal investigations. In all three jurisdictions, investigators must generally demonstrate that digital evidence has been lawfully obtained, properly preserved, and reliably analyzed. Procedural requirements commonly include judicial authorization for searches and seizures, documentation of forensic acquisition methods, maintenance of chain of custody, and expert testimony regarding technical findings. Courts typically evaluate whether electronic evidence satisfies standards of relevance, authenticity, integrity, and reliability before admitting it into evidence. Recent technological developments have increased the complexity of procedural requirements. Digital investigations now frequently involve cloud servers, encrypted devices, remote data storage, and international service providers. Consequently, criminal procedure laws face growing pressure to address issues such as remote searches, cross-border evidence requests, digital surveillance, and AI-assisted forensic analysis. Ensuring procedural consistency in these areas remains a major challenge for contemporary criminal justice systems.[19]

Comparative Legislative Overview

A comparative analysis reveals that Pakistan, Indonesia, and Malaysia share several common objectives, including the legal recognition of electronic evidence, the criminalization of cyber-related offenses, and the development of investigative mechanisms for obtaining digital data. All three jurisdictions acknowledge the growing importance of digital evidence and have adopted legislative measures designed to facilitate its use in criminal proceedings. Nevertheless, important differences exist. Malaysia possesses a relatively mature evidentiary framework supported by extensive judicial interpretation and specialized legislation addressing electronic records. Indonesia has developed a comprehensive digital governance regime through its Electronic Information and Transactions Law, which provides a broad foundation for the admissibility of electronic evidence. Pakistan has made significant progress through PECA and electronic transaction legislation but continues to face challenges relating to implementation, forensic capacity, and procedural consistency. From a contemporary perspective, all three legal systems confront similar emerging issues, including artificial intelligence-generated evidence, deepfake technologies, encrypted communications, cloud-based storage, and transnational cybercrime. Existing legislative frameworks were largely designed before the widespread adoption of many of these technologies and therefore require ongoing adaptation. Greater harmonization of evidentiary standards, enhanced forensic capabilities, improved judicial training, and strengthened international

[19] Gul, S., Ahmad, F., & Ahmad, R. (2025). Digital evidence and procedural fairness: Reforming cybercrime prosecution in Pakistan. *Journal for Social Science Archives*, *3*(2), 544–554. https://doi.org/10.59075/jssa.v3i2.260

cooperation will be essential to ensuring the effective use of digital evidence in criminal proceedings.

Overall, the comparative experience of Pakistan, Indonesia, and Malaysia demonstrates both significant progress and persistent challenges in regulating digital evidence. As technological innovation continues to reshape criminal activity and investigative practices, legal systems must develop increasingly sophisticated regulatory frameworks capable of balancing evidentiary reliability, effective law enforcement, procedural fairness, and the protection of fundamental rights.[20]

LEGAL CHALLENGES IN THE ADMISSION AND EVALUATION OF DIGITAL EVIDENCE

The increasing reliance on digital evidence in criminal investigations has transformed the administration of justice across the world. Electronic records, social media communications, cloud-based data, surveillance footage, mobile device extractions, and blockchain transactions have become essential sources of evidence in modern criminal proceedings. Despite their evidentiary value, digital materials present unique legal and technical challenges that differ substantially from traditional forms of evidence. The admissibility and evaluation of digital evidence require courts to address complex questions relating to authenticity, integrity, reliability, privacy, cybersecurity, and jurisdiction. These challenges have become even more significant in the contemporary era characterized by artificial intelligence (AI), deepfake technologies, encrypted communications, and transnational cybercrime.[21]

Authenticity and Integrity Concerns

One of the most fundamental challenges in the admission of digital evidence is establishing authenticity and integrity. Authenticity refers to the ability to demonstrate that the evidence is genuinely what it purports to be, while integrity concerns whether the evidence has remained complete and unaltered throughout the investigative process. Unlike physical evidence, digital information can be copied, modified, deleted, or manipulated without leaving visible traces. Consequently, courts must be satisfied that electronic records accurately represent the original information and have not been compromised. The

[20] Mujiono, & Ticualu, C. (2025). Emerging trends in law and social sciences: Global perspectives on policy, ethics, justice, and institutional reform. *International Journal of Law and Social Sciences*, *1*(1), 40–60. https://doi.org/10.65960/ijlss.1.1.2025.6

[21] Anggraeniko, L. S., Ambarwati, A., & Utami, F. R. (2026). Admissibility of digital evidence in Indonesia: Criminal–civil implications for the chain of custody and evidentiary validity. *Priviet Social Sciences Journal*, *6*(4), 168–177. https://doi.org/10.55942/pssj.v6i4.1566

challenge of authenticity has become increasingly complex with the proliferation of cloud computing and remote data storage. Digital evidence often passes through multiple devices, networks, and service providers before reaching investigators. Establishing a clear evidentiary trail requires sophisticated forensic procedures, including metadata analysis, hash-value verification, forensic imaging, and detailed chain-of-custody documentation. Any gaps in these processes may undermine the evidentiary value of the material and raise doubts regarding its reliability. In Pakistan, Indonesia, and Malaysia, courts increasingly rely on forensic experts to authenticate electronic records. However, disparities in technical expertise, forensic infrastructure, and judicial familiarity with digital technologies may result in inconsistent evidentiary assessments. As criminal investigations become more technologically sophisticated, ensuring the authenticity and integrity of digital evidence remains one of the most pressing challenges facing modern criminal justice systems.[22]

Digital Forgery and Manipulation

A major contemporary threat to the reliability of digital evidence is the growing sophistication of digital forgery and manipulation technologies. Advances in artificial intelligence have enabled the creation of highly realistic synthetic media, commonly referred to as deepfakes. These technologies can generate fabricated audio recordings, videos, photographs, and documents that closely resemble authentic materials. As a result, distinguishing genuine evidence from manipulated content has become increasingly difficult. Deepfake technology presents serious implications for criminal proceedings. Fabricated video recordings may falsely implicate individuals in criminal activities, while manipulated audio files can distort conversations or create false confessions. Similarly, altered digital documents may be used to conceal fraud, corruption, or financial crimes. Traditional methods of visual inspection are often insufficient to detect sophisticated digital manipulations, necessitating the use of advanced forensic techniques and expert analysis. The emergence of generative artificial intelligence has further complicated evidentiary evaluation. AI tools can now produce highly convincing text, images, voice recordings, and videos at relatively low cost. This development raises important legal questions regarding evidentiary presumptions, burdens of proof, and standards of authentication. Courts may increasingly require independent technical verification before accepting digital media as reliable evidence.[23]

---

[22] Azhari, A. M., Azhari, S., & Yaqooq, M. I. (2025). Global transformations in law, justice, and society: Comparative perspectives on governance, rights, and legal reform. *International Journal of Law and Social Sciences*, *1*(1), 60–90. https://doi.org/10.65960/ijlss.1.1.2025.7

[23] Saeed, A., & Adhi, B. Z. (2025). Digital forensics and fair trial rights in Pakistan: Legal, procedural, and institutional challenges in cybercrime prosecutions. *Contemporary Journal of Social Science Review*, *3*(2), 488–499. https://doi.org/10.63878/cjssr.v3i2.1969

Cybersecurity Vulnerabilities

Cybersecurity vulnerabilities represent another significant challenge in the collection and preservation of digital evidence. Criminal investigations frequently involve computer systems, mobile devices, cloud servers, and digital networks that may themselves be vulnerable to cyberattacks. Unauthorized access, malware infections, ransomware attacks, and data breaches can compromise the reliability of electronic evidence and raise concerns regarding evidentiary contamination. The increasing use of interconnected technologies has expanded the attack surface available to cybercriminals. Evidence stored on cloud platforms may be exposed to unauthorized access from remote actors, while poorly secured databases may become vulnerable to manipulation. In some cases, investigators themselves may inadvertently alter digital evidence through improper handling procedures or inadequate cybersecurity safeguards. Cybersecurity risks are particularly concerning in cases involving critical infrastructure, financial institutions, government systems, and national security matters. If digital evidence is obtained from compromised systems, courts may question whether the data accurately reflects the underlying events. Establishing evidentiary reliability therefore requires not only forensic verification but also assurances regarding the security of the systems from which the evidence was obtained. Recent increases in ransomware attacks and cyber intrusions demonstrate the practical significance of these concerns. Law enforcement agencies worldwide have encountered situations where digital evidence was encrypted, corrupted, or rendered inaccessible by malicious actors. These developments highlight the need for comprehensive cybersecurity protocols throughout the evidence collection, preservation, and analysis process.[24]

Privacy and Data Protection Issues

The growing use of digital evidence also raises significant concerns regarding privacy rights and data protection. Modern digital devices contain vast quantities of personal information, including communications, photographs, browsing histories, location data, financial records, health information, and social media activity. Accessing such information during criminal investigations may involve substantial intrusions into individual privacy. Balancing effective law enforcement with the protection of fundamental rights has become a central challenge in contemporary criminal procedure. Investigators often seek access to smartphones, encrypted messaging applications, cloud storage accounts, and

[24] Al-Farjani, S. H., Ahmad, T., & Rana, H. A. S. (2025). Digital innovation, legal reform, and social justice: Interdisciplinary approaches to law, technology, and human rights. *International Journal of Law and Social Sciences*, *1*(1), 91–129. https://doi.org/10.65960/ijlss.1.1.2025.5

digital communication platforms. While such access may be necessary to investigate criminal conduct, it also creates risks of excessive surveillance and unauthorized collection of personal information.

The expansion of digital surveillance technologies has intensified these concerns. Governments increasingly utilize facial recognition systems, biometric databases, predictive analytics, and AI-assisted monitoring tools to identify suspects and prevent criminal activities. Although these technologies may enhance public security, they also raise questions regarding proportionality, transparency, accountability, and the potential misuse of personal data. Data protection legislation in many jurisdictions seeks to regulate the collection, processing, and retention of personal information. Nevertheless, tensions frequently arise between privacy protections and investigative requirements. Courts must therefore carefully assess whether digital evidence has been obtained through lawful and proportionate means consistent with constitutional guarantees and human rights standards.

In Pakistan, Indonesia, and Malaysia, legal debates surrounding privacy rights continue to evolve alongside technological developments. The increasing use of cloud services, cross-border data transfers, and AI-driven surveillance systems requires legal frameworks capable of balancing competing interests while safeguarding individual liberties.[25]

Jurisdictional and Cross-Border Challenges

Digital evidence frequently transcends national borders, creating complex jurisdictional challenges for criminal investigations. Unlike traditional evidence, electronic data may be stored on servers located in multiple countries, transmitted through international networks, and controlled by foreign service providers. Consequently, determining which legal system governs access to digital evidence can be highly complicated. Cross-border cybercrime investigations often require cooperation among multiple jurisdictions. Law enforcement authorities may need access to evidence held by multinational technology companies, cloud service providers, or social media platforms operating outside their territorial jurisdiction. Obtaining such evidence typically involves mutual legal assistance procedures, international agreements, and diplomatic cooperation, all of which can be time-consuming and procedurally burdensome. The widespread use of encrypted communication platforms further complicates cross-border investigations. Messaging applications employing end-to-end encryption frequently store limited user data, making it difficult for investigators to access relevant evidence even when legal

[25] Noor, S., Azeem, A., & Maqsood, W. (2025). Enhancing forensic evidence management in Pakistan's criminal justice system: A criminological analysis. *Journal of Political Stability Archive*, *3*(4), 184–195. https://doi.org/10.63468/jpsa.3.4.26

authorization exists. Additionally, differing national laws regarding privacy, data retention, and government access create inconsistencies that hinder effective international cooperation.

Emerging technologies such as blockchain and decentralized networks present additional jurisdictional difficulties. Cryptocurrency transactions often involve participants located in multiple countries and may be recorded on distributed ledgers that lack a central authority. Determining jurisdiction, identifying suspects, and securing admissible evidence in such cases remains a significant challenge for contemporary legal systems. For Pakistan, Indonesia, and Malaysia, these issues are particularly relevant due to the increasing prevalence of transnational cybercrime, online fraud, financial crimes, and digital communication networks. Strengthening regional cooperation mechanisms, harmonizing evidentiary standards, and developing efficient cross-border data access procedures will be essential to addressing these challenges effectively.[26]

COMPARATIVE ANALYSIS OF JUDICIAL PRACTICE AND EVIDENTIARY STANDARDS

The increasing reliance on digital evidence in criminal investigations has significantly influenced judicial practice across Pakistan, Indonesia, and Malaysia. Courts in these jurisdictions are increasingly required to evaluate electronic communications, digital documents, social media content, mobile phone records, surveillance footage, cloud-based data, and other forms of electronically stored information. While legislative reforms have provided legal recognition to digital evidence, judicial interpretation remains crucial in determining how evidentiary standards are applied in practice. The comparative examination of judicial approaches reveals both convergence and divergence regarding authenticity, reliability, admissibility, and procedural safeguards. Furthermore, contemporary developments such as artificial intelligence (AI), deepfake technology, encrypted communications, and cross-border cybercrime have introduced new challenges that existing judicial frameworks must address.[27]

Case Law Analysis from Pakistan

Pakistani courts have progressively recognized the evidentiary value of electronic records and digital communications. Judicial decisions have generally

[26] Al Azhari, F. U., & Al Azhari, S. I. (2025). Contemporary challenges in harmonizing Sharia, national legal systems, and international law in a rapidly changing world. *International Journal of Law and Social Sciences*, *1*(1), 130–150. https://doi.org/10.65960/ijlss.1.1.2025.4

[27] Dhumillah, D. S. R. (2024). The stand of electronic evidence in cyber crime law enforcement in Indonesia. *Eduvest - Journal of Universal Studies*, *4*(9), 4215–4226. https://doi.org/10.59188/eduvest.v4i9.1812

emphasized that digital evidence is admissible provided that its authenticity, relevance, and reliability can be established. Courts frequently rely on provisions contained within the Qanun-e-Shahadat Order, the Electronic Transactions Ordinance, and the Prevention of Electronic Crimes Act (PECA) to evaluate electronic evidence. A recurring theme in Pakistani jurisprudence is the requirement that digital evidence be supported by adequate forensic verification. Courts have demonstrated caution when assessing electronic communications such as emails, text messages, call records, and social media content, often requiring corroborating evidence to establish reliability. Judicial decisions have also highlighted the importance of maintaining an unbroken chain of custody and ensuring that digital evidence has not been altered or manipulated. Recent cybercrime prosecutions have demonstrated growing judicial awareness of technological complexities. Courts increasingly recognize that electronic evidence may constitute the primary source of proof in cases involving online fraud, cyber harassment, identity theft, financial crimes, and terrorism-related offenses. However, challenges remain due to variations in forensic expertise, inconsistent evidentiary practices, and limited judicial training in digital forensics. As technologies such as AI-generated content and encrypted communications become more prevalent, Pakistani courts face increasing pressure to develop more sophisticated evidentiary standards.[28]

Case Law Analysis from Indonesia

Indonesian courts have played a significant role in interpreting the Electronic Information and Transactions Law (ITE Law), which recognizes electronic information and electronic documents as valid forms of legal evidence. Judicial practice has generally adopted an expansive approach toward the admissibility of digital evidence, reflecting Indonesia's broader commitment to digital governance and electronic transactions. Indonesian courts frequently admit electronic communications, social media posts, digital contracts, and electronic records in both criminal and civil proceedings. In evaluating such evidence, judges typically focus on authenticity, integrity, and procedural legality. Digital forensic reports often serve as an important mechanism for establishing evidentiary reliability. A notable aspect of Indonesian judicial practice is the increasing use of social media evidence in criminal prosecutions involving online defamation, hate speech, cybercrime, and misinformation. As digital platforms have become central to public discourse, courts have encountered complex questions concerning freedom of expression, privacy rights, and evidentiary authenticity. Judicial decisions increasingly require technical verification of electronic content to ensure that digital materials have not been manipulated. Recent developments involving artificial intelligence, digital surveillance

[28] Siswanto, M. A., & Ahmad, T. (2026). Climate justice in Islamic legal thought: Harmonizing environmental law, human rights, and sustainable development in OIC countries. *International Journal of Law and Social Sciences, 2*(1), 20–41. https://doi.org/10.65960/ijlss.2.1.2026.14

technologies, and cross-border cybercrime have further challenged Indonesian courts. The growing prevalence of encrypted communications and cloud-based services has complicated efforts to obtain and authenticate electronic evidence. Consequently, judicial practice continues to evolve in response to emerging technological realities and the need to balance effective law enforcement with constitutional protections.[29]

Case Law Analysis from Malaysia

Malaysia possesses one of the most developed judicial frameworks concerning digital evidence in Southeast Asia. Malaysian courts have accumulated substantial experience in interpreting provisions of the Evidence Act, the Computer Crimes Act, and related legislation governing electronic records and cybercrime. This extensive jurisprudence has contributed to greater legal certainty regarding the admissibility and evaluation of digital evidence. Malaysian courts generally adopt a pragmatic approach toward electronic evidence while emphasizing procedural safeguards designed to ensure authenticity and reliability. Computer-generated records, electronic communications, surveillance footage, and digital forensic reports are routinely admitted when supported by appropriate evidentiary foundations. Judicial decisions frequently underscore the importance of expert testimony, forensic validation, and chain-of-custody documentation. One of the strengths of Malaysian jurisprudence is its relatively sophisticated treatment of technical evidentiary issues. Courts have demonstrated willingness to engage with complex forensic methodologies and technological concepts when evaluating electronic evidence. This approach has facilitated the effective prosecution of cybercrime, financial fraud, and technology-related offenses. Nevertheless, Malaysian courts face challenges similar to those encountered in other jurisdictions. The emergence of AI-generated content, deepfake technologies, blockchain transactions, and encrypted messaging platforms raises novel evidentiary questions that existing legal frameworks were not originally designed to address. As digital technologies continue to evolve, Malaysian jurisprudence must adapt to maintain evidentiary reliability and procedural fairness.[30]

Comparative Assessment of Judicial Approaches

[29] Costa, V. V. da, Costa, C. da, Cristovao, R. J., Cruz, C. da, & Pinto, F. C. (2026). *Reconstruction of regulation for corruption eradication commission officers involved in corruption cases base on justice values. International Journal of Law and Social Sciences, 2*(1). https://doi.org/10.65960/ijlss.2.1.2026.10

[30] Satyo, B. K., & Prasetyo, B. A. Y. (2026). *Artificial intelligence and the future of human rights: Legal accountability for algorithmic decision-making in democratic societies. International Journal of Law and Social Sciences, 2*(1), 54–74. https://doi.org/10.65960/ijlss.2.1.2026.12

A comparative analysis of judicial practice reveals several common trends across Pakistan, Indonesia, and Malaysia. First, courts in all three jurisdictions recognize the legal validity of digital evidence and increasingly rely upon electronic records in criminal proceedings. Second, authenticity and reliability remain the primary considerations in determining admissibility. Third, digital forensic expertise plays an increasingly important role in judicial decision-making. Despite these similarities, significant differences exist regarding the maturity and consistency of judicial approaches. Malaysian courts generally exhibit the highest degree of institutional experience in handling digital evidence, supported by extensive legislative guidance and judicial precedent. Indonesian courts have adopted a broad and flexible approach to electronic evidence but continue to confront challenges relating to privacy protection, online expression, and technological complexity. Pakistani courts have made substantial progress in recognizing digital evidence but face ongoing difficulties associated with forensic capacity, procedural consistency, and specialized judicial training.[31]

Strengths and Weaknesses of Existing Systems

The existing systems possess several notable strengths. Legislative recognition of electronic evidence has enabled courts to respond more effectively to contemporary forms of criminal activity. Judicial willingness to consider digital evidence has improved the prosecution of cybercrime, financial fraud, corruption, and technology-enabled offenses. Furthermore, increasing reliance on forensic expertise has enhanced evidentiary reliability and investigative effectiveness. However, important weaknesses remain. One recurring challenge is the uneven availability of digital forensic resources. Investigative agencies and courts may lack access to advanced forensic technologies, specialized laboratories, and trained personnel. These limitations can undermine the accuracy and consistency of evidentiary assessments. Another weakness involves the rapid pace of technological change. Existing laws and judicial doctrines often lag behind innovations such as generative artificial intelligence, blockchain systems, decentralized networks, and quantum computing technologies. Consequently, courts may struggle to apply traditional evidentiary principles to novel digital environments. Cross-border investigations also expose structural weaknesses in current legal frameworks. Digital evidence frequently resides outside national jurisdictions, creating procedural delays and legal uncertainty. Differences in privacy regulations, data protection standards, and evidentiary requirements further complicate international cooperation.[32]

---

[31] Mustafa, A., Ishaque, M., Raza, R., Samiullah, & Raza, M. I. (2025). When culture meets Fiqh: Examining the legal authority of ʿUrf in contemporary engagement traditions. *Global Islamic Research Journal*, *1*(1), 1–21. https://doi.org/10.65960/girj.1.1.2025.6

[32] Al Azhari, F. U., Shah, S. H. M., Al Azhari, S. I., Rasool, F., Ahmed, R., Samad, A., & Rehman, A. (2025). The role of Islamic economic principles in family law: A study on inheritance and property rights within the

Lessons from International Best Practices

The experiences of advanced digital jurisdictions and international organizations provide valuable lessons for Pakistan, Indonesia, and Malaysia. International best practices emphasize the importance of forensic standardization, judicial specialization, technological capacity-building, and cross-border cooperation.

First, legal systems should adopt internationally recognized digital forensic standards governing evidence acquisition, preservation, authentication, and analysis. Standardized procedures enhance evidentiary reliability and facilitate international cooperation.

Second, specialized judicial training programs are essential for improving the ability of judges, prosecutors, and defense lawyers to evaluate complex technological evidence. As digital investigations increasingly involve artificial intelligence, encryption, blockchain technologies, and cybersecurity issues, legal professionals require greater technical literacy.

Third, stronger regional and international cooperation mechanisms are necessary to address transnational cybercrime and cross-border evidence requests. Harmonized evidentiary standards can reduce procedural barriers and improve investigative efficiency.

Finally, legal frameworks should proactively address emerging technologies rather than merely responding to technological developments after they occur. Regulatory approaches must incorporate safeguards relating to AI-generated evidence, deepfake detection, algorithmic transparency, and digital privacy protection. Such measures will help preserve public confidence in the integrity of digital evidence and the fairness of criminal proceedings.[33]

TOWARDS A HARMONIZED FRAMEWORK FOR DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS

The rapid expansion of digital technologies has transformed criminal investigations and judicial processes across the globe. Digital evidence now plays a central role in prosecuting cybercrime, financial fraud, terrorism, corruption, human trafficking, and other transnational offenses. However, the increasing

context of child protection. *Global Islamic Research Journal*, *1*(1), 59–76. https://doi.org/10.65960/girj.1.1.2025.2

[33] Zubair, A. A., Salman, K., & Zakariyyah, A. O. (2026). Existing legal and regulatory framework for sovereign Sukuk in Nigeria. *Global Islamic Research Journal, 2*(1), 36–73. https://doi.org/10.65960/girj.2.1.2026.8

complexity of digital ecosystems has exposed significant legal, procedural, and technical challenges that individual states often struggle to address independently. Differences in evidentiary standards, investigative procedures, forensic capabilities, and data governance frameworks create obstacles to the effective collection, authentication, and admission of digital evidence. These challenges are particularly pronounced in Pakistan, Indonesia, and Malaysia, where legal systems are actively adapting to technological innovation while attempting to preserve due process and fundamental rights. Consequently, there is a growing need for a harmonized framework capable of facilitating cross-border cooperation, ensuring evidentiary reliability, and responding to emerging technological developments such as artificial intelligence (AI), deepfake technologies, blockchain systems, and cloud computing.[34]

Need for Legal Harmonization

The transnational nature of digital evidence necessitates greater legal harmonization among states. Unlike traditional forms of evidence, electronic data frequently crosses national boundaries and may be stored on servers located in multiple jurisdictions. Criminal investigations increasingly involve multinational technology companies, cloud service providers, encrypted communication platforms, and decentralized digital networks. In such circumstances, inconsistencies between national legal frameworks can significantly impede the efficient collection and admissibility of evidence.

Pakistan, Indonesia, and Malaysia have each adopted legislative measures governing electronic evidence and cybercrime. However, important differences remain regarding evidentiary thresholds, data retention obligations, investigative powers, privacy protections, and forensic procedures. These divergences create uncertainty for investigators, prosecutors, judges, and digital service providers operating across borders. Furthermore, differing procedural requirements may delay criminal proceedings and complicate international cooperation. Legal harmonization does not require complete uniformity. Rather, it involves establishing common minimum standards governing the acquisition, preservation, authentication, and presentation of digital evidence. Such harmonization would facilitate mutual recognition of digital evidence, enhance judicial cooperation, and improve the effectiveness of cross-border criminal investigations. Given the increasing prevalence of transnational cybercrime, regional coordination has become a practical necessity rather than a purely academic objective.

Proposed Evidentiary Standards

[34] Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs*, *3*(5), 112–124. https://doi.org/10.71317/rjsa.003.05.0375

A harmonized framework should establish clear and uniform evidentiary standards capable of ensuring the reliability and admissibility of digital evidence. These standards should be grounded in internationally recognized principles of authenticity, integrity, relevance, reliability, and legality.

First, digital evidence should be presumed admissible only when supported by verifiable authentication procedures. Authentication should include forensic verification, metadata analysis, cryptographic validation, and documentation demonstrating the origin and integrity of electronic records. The use of cryptographic hash values should become a mandatory component of digital evidence preservation to ensure that evidence remains unaltered throughout the investigative process.

Second, standardized chain-of-custody requirements should be implemented across jurisdictions. Every stage of evidence collection, transfer, storage, examination, and presentation should be documented to maintain evidentiary integrity. Such procedures reduce opportunities for tampering and increase judicial confidence in digital evidence.

Third, legal frameworks should establish specific standards for evaluating AI-generated and synthetic digital content. As deepfake technologies become increasingly sophisticated, traditional evidentiary methods may no longer be sufficient. Courts should require enhanced forensic verification for digital audio, video, and image evidence where manipulation is reasonably suspected.

Finally, evidentiary standards should incorporate principles of transparency and explainability, particularly when artificial intelligence systems are utilized in digital forensic analysis. Judges and litigants must be able to understand and challenge the methodologies used to generate forensic conclusions.[35]

Strengthening Forensic Capabilities

The effectiveness of digital evidence regulation depends heavily upon the availability of advanced forensic capabilities. Even the most sophisticated legal framework cannot function effectively if investigative agencies lack the technical resources necessary to collect, preserve, and analyze electronic data. Pakistan, Indonesia, and Malaysia have made significant investments in digital forensic infrastructure; however, disparities remain regarding institutional capacity and technological resources. Strengthening forensic capabilities requires the

[35] Abood, T. A., Dakhil, M. H., Nasef, A. J., Abed, A. Q., & Hamid, A. K. (2026). Authority and interpretation in Qur'anic studies: Re-examining classical tafsīr in contemporary Islamic scholarship. *Global Islamic Research Journal, 2*(1), 1–17. https://doi.org/10.65960/girj.2.1.2026.10

establishment of specialized digital forensic laboratories equipped with modern technologies capable of handling emerging forms of digital evidence. These facilities should possess expertise in mobile device forensics, cloud forensics, network analysis, blockchain investigations, malware analysis, and AI-assisted forensic examination.

In addition, governments should adopt internationally recognized forensic standards to ensure consistency and reliability. Standardized forensic procedures reduce the likelihood of evidentiary contamination and facilitate cross-border cooperation. Accreditation systems should also be implemented to ensure that forensic laboratories maintain high levels of professional competence and technical accuracy.

Investment in research and innovation is equally important. Emerging technologies such as quantum computing, decentralized finance, generative AI, and Internet-of-Things devices will create new evidentiary challenges that require continuous adaptation of forensic methodologies. Sustainable forensic capacity-building therefore demands long-term institutional commitment rather than temporary technological solutions.[36]

Judicial and Prosecutorial Training

The increasing complexity of digital evidence has transformed the role of judges and prosecutors within criminal justice systems. Contemporary criminal proceedings frequently involve sophisticated technical concepts that extend beyond traditional legal expertise. Consequently, judicial and prosecutorial training has become an essential component of any harmonized framework. Judges must possess sufficient technological literacy to evaluate expert testimony, assess forensic methodologies, and determine evidentiary reliability. Without such knowledge, courts may struggle to distinguish between credible scientific analysis and unsupported technical claims. Similarly, prosecutors require specialized training to understand digital investigations, manage electronic evidence, and effectively present forensic findings during trial proceedings. Training programs should address emerging issues such as artificial intelligence, machine learning, blockchain technologies, cryptocurrency transactions, cloud computing, cybersecurity, and digital privacy. Particular attention should be devoted to the evidentiary implications of deepfake technologies and AI-generated content, which are likely to become increasingly common in future litigation. Judicial academies, law enforcement institutions, and universities should collaborate to develop interdisciplinary educational programs that integrate legal, technological, and forensic perspectives.

[36] Alwan, F. Y., & Lilo, I. Y. (2026). Defending religious tradition in modern times: Comparative responses of Muslim and Christian scholars to scriptural criticism. *Global Islamic Research Journal, 2*(1), 18–35. https://doi.org/10.65960/girj.2.1.2026.11

Continuous professional development will be essential as technological innovation continues to reshape evidentiary practices.[37]

CONCLUSION

The increasing reliance on digital technologies has fundamentally transformed criminal investigations and judicial proceedings, making digital evidence an indispensable component of modern criminal justice systems. This study examined the legal foundations, regulatory frameworks, evidentiary challenges, and judicial practices relating to digital evidence in Pakistan, Indonesia, and Malaysia. The findings demonstrate that all three jurisdictions have recognized the legal validity of electronic evidence and have enacted legislative measures to address cybercrime and digital investigations. However, significant challenges remain concerning the authentication, integrity, admissibility, and evaluation of digital evidence, particularly in light of emerging technologies such as artificial intelligence, deepfakes, cloud computing, blockchain systems, and encrypted communications.

The comparative analysis reveals both convergence and divergence among the selected jurisdictions. Malaysia possesses a relatively mature legal and judicial framework supported by extensive jurisprudence and specialized legislation governing electronic evidence. Indonesia has developed a comprehensive regulatory structure through its Electronic Information and Transactions Law, while Pakistan has made substantial progress through the Prevention of Electronic Crimes Act and related legal reforms. Nevertheless, all three countries face common challenges relating to forensic capacity, judicial expertise, cybersecurity threats, privacy protection, and cross-border evidence collection.

This study contributes to the field of criminal procedure law by highlighting the need for harmonized evidentiary standards capable of addressing contemporary technological realities. It demonstrates that effective regulation of digital evidence requires not only legislative recognition but also robust forensic procedures, judicial competence, procedural safeguards, and international cooperation. The proposed framework offers practical guidance for strengthening the reliability, admissibility, and evidentiary value of digital evidence within criminal proceedings.

Future research should explore the legal implications of emerging technologies, particularly AI-generated evidence, algorithmic decision-making,

[37] Cami, G. (2024). Legal standards for cross-border access to electronic evidence in criminal procedure: An Albanian perspective on international standards. *Studia Iuridica Lublinensia*, *33*(5), 11–30. https://doi.org/10.17951/sil.2024.33.5.11-30

quantum computing, and decentralized digital infrastructures. Further comparative studies involving additional Muslim-majority jurisdictions and international legal systems would also provide valuable insights into the development of globally compatible standards for digital evidence. As technology continues to evolve, ongoing scholarly engagement will remain essential to ensuring that criminal justice systems effectively balance innovation, evidentiary reliability, and the protection of fundamental rights.

References

1. Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs*, *3*(5). https://doi.org/10.71317/rjsa.003.05.0375
2. Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. In *Proceedings - 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)* (pp. 11–20). IEEE. https://doi.org/10.1109/tps-isa62245.2024.00012
3. Romaniuk, V., & Ablamskyi, S. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law and Safety*, (2), 143–152. https://doi.org/10.32631/pb.2024.2.13
4. Petryk, V. V. (2025). Vykorystannia elektronnykh dokaziv u kryminalnomu provadzhenni: problemy yikh zboru, perevirky ta otsinky [The use of electronic evidence in criminal proceedings: issues of collection, verification, and evaluation]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo* [*Uzhhorod National University Herald. Series: Law*], *87*(4), 119–123. https://doi.org/10.24144/2307-3322.2025.87.4.17
5. Shyshenko, A. O. (2025). Tsyfrovye dokazy u kryminalnomu provadzhenni: problemy avtentychnosti ta dopustymosti [Digital evidences in criminal proceedings: problems of authenticity and admissibility]. *Analitychno-Porivnialne Pravoznavstvo* [*Analytical and Comparative Jurisprudence*], *5*(3), 312–316. https://doi.org/10.24144/2788-6018.2025.05.3.46
6. Matis, J. (2024). Certain aspects of criminal evidence and digital evidence. *Analytical and Comparative Jurisprudence*, (2), 701–705. https://doi.org/10.24144/2788-6018.2024.02.116
7. Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, *16*(2), 23–44. https://doi.org/10.22201/iij.24485306e.2024.2.18892

8. Luhina, N., & Paliukh, O. (2025). Peculiarities of proof in criminal proceedings related to cybercrime. *Social Development: Economic and Legal Issues*, (4), 205–214. https://doi.org/10.70651/3083-6018/2025.4.27
9. Didenko, O. V. (2025). Tsyfrova kryminalistyka ta mizhnarodna protydiia kiberzlochynnosti (na prykladi elektronnoi komertsii) [Digital forensics and international counteraction to cybercrime (based on the example of e-commerce)]. *Analitychno-Porivnialne Pravoznavstvo* [*Analytical and Comparative Jurisprudence*], *4*(3), 162–167. https://doi.org/10.24144/2788-6018.2025.04.3.26
10. Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs*, *3*(5). https://doi.org/10.71317/rjsa.003.05.0375
11. Asgarova, M. P., Aliyev, B. A. O., Khalilov, F. Y., & Hasanova, I. Z. K. (2022). The use of electronic evidence in court: A comparative legal analysis in the world practice. *Cuestiones Políticas*, *40*(72), 373–388. https://doi.org/10.46398/cuestpol.4072.21
12. Osco Escobedo, M. A., Chipana Fernández, Y. M. M., Quiñones Li, A. E., Díaz-Pérez, J. J., Calvo de Oliveira Diaz, D. G., & Garcia Quispe, G. B. (2023). Digital evidence as a means of proof in criminal proceedings. *Russian Law Journal*, *11*(5s). https://doi.org/10.52783/rlj.v11i5s.895
13. Ahmadian, M. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, *11*(1), Article 19. https://doi.org/10.1186/s41935-021-00234-6
14. Rashkovsk, D., & Rashkovska, V. (2025). The difference between digital evidence and evidence in digital form. *Iustinianus Primus Law Review*, *16*(2), 68–79. https://doi.org/10.55302/iplr2516268r
15. Zahoor, R., Waqar Khan Arif, S. M., & Bannian, B. (2022). Digital evidence and its admissibility under Pakistani law. *Journal of Development and Social Sciences*, *3*(4), 51–60. https://doi.org/10.47205/jdss.2022(3-iv)06
16. Dhumillah, D. S. R. (2024). The stand of electronic evidence in cyber crime law enforcement in Indonesia. *Eduvest - Journal of Universal Studies*, *4*(9), 4215–4226. https://doi.org/10.59188/eduvest.v4i9.1812
17. D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The chain of custody in the era of modern forensics: From the classic procedures for gathering evidence to the new challenges related to digital data. *Healthcare*, *11*(5), Article 634. https://doi.org/10.3390/healthcare11050634
18. Hasanah, L. N., Faisal, M. S., Ahmed, Z., & Hasyim, M. Y. A. (2025). Religious diversity and the digital economy: Legal–academic pathways to

harmonize Sharia and international law. *International Journal of Law and Social Sciences*, *1*(1). https://doi.org/10.65960/ijlss.1.1.2025.8

19. Gul, S., Ahmad, F., & Ahmad, R. (2025). Digital evidence and procedural fairness: Reforming cybercrime prosecution in Pakistan. *Journal for Social Science Archives*, *3*(2), 544–554. https://doi.org/10.59075/jssa.v3i2.260
20. Mujiono, & Ticualu, C. (2025). Emerging trends in law and social sciences: Global perspectives on policy, ethics, justice, and institutional reform. *International Journal of Law and Social Sciences*, *1*(1), 40–60. https://doi.org/10.65960/ijlss.1.1.2025.6
21. Anggraeniko, L. S., Ambarwati, A., & Utami, F. R. (2026). Admissibility of digital evidence in Indonesia: Criminal–civil implications for the chain of custody and evidentiary validity. *Priviet Social Sciences Journal*, *6*(4), 168–177. https://doi.org/10.55942/pssj.v6i4.1566
22. Azhari, A. M., Azhari, S., & Yaqooq, M. I. (2025). Global transformations in law, justice, and society: Comparative perspectives on governance, rights, and legal reform. *International Journal of Law and Social Sciences*, *1*(1), 60–90. https://doi.org/10.65960/ijlss.1.1.2025.7
23. Saeed, A., & Adhi, B. Z. (2025). Digital forensics and fair trial rights in Pakistan: Legal, procedural, and institutional challenges in cybercrime prosecutions. *Contemporary Journal of Social Science Review*, *3*(2), 488–499. https://doi.org/10.63878/cjssr.v3i2.1969
24. Al-Farjani, S. H., Ahmad, T., & Rana, H. A. S. (2025). Digital innovation, legal reform, and social justice: Interdisciplinary approaches to law, technology, and human rights. *International Journal of Law and Social Sciences*, *1*(1), 91–129. https://doi.org/10.65960/ijlss.1.1.2025.5
25. Noor, S., Azeem, A., & Maqsood, W. (2025). Enhancing forensic evidence management in Pakistan's criminal justice system: A criminological analysis. *Journal of Political Stability Archive*, *3*(4), 184–195. https://doi.org/10.63468/jpsa.3.4.26
26. Al Azhari, F. U., & Al Azhari, S. I. (2025). Contemporary challenges in harmonizing Sharia, national legal systems, and international law in a rapidly changing world. *International Journal of Law and Social Sciences*, *1*(1), 130–150. https://doi.org/10.65960/ijlss.1.1.2025.4
27. Dhumillah, D. S. R. (2024). The stand of electronic evidence in cyber crime law enforcement in Indonesia. *Eduvest - Journal of Universal Studies*, *4*(9), 4215–4226. https://doi.org/10.59188/eduvest.v4i9.1812
28. Siswanto, M. A., & Ahmad, T. (2026). Climate justice in Islamic legal thought: Harmonizing environmental law, human rights, and sustainable development in OIC countries. *International Journal of Law and Social Sciences, 2*(1), 20–41. https://doi.org/10.65960/ijlss.2.1.2026.14
29. Costa, V. V. da, Costa, C. da, Cristovao, R. J., Cruz, C. da, & Pinto, F. C. (2026). *Reconstruction of regulation for corruption eradication commission officers involved in corruption cases base on justice values*. *International Journal of Law and Social Sciences, 2*(1). https://doi.org/10.65960/ijlss.2.1.2026.10

30. Satyo, B. K., & Prasetyo, B. A. Y. (2026). *Artificial intelligence and the future of human rights: Legal accountability for algorithmic decision-making in democratic societies. International Journal of Law and Social Sciences, 2*(1), 54–74. https://doi.org/10.65960/ijlss.2.1.2026.12
31. Mustafa, A., Ishaque, M., Raza, R., Samiullah, & Raza, M. I. (2025). When culture meets Fiqh: Examining the legal authority of ʿUrf in contemporary engagement traditions. *Global Islamic Research Journal*, *1*(1), 1–21. https://doi.org/10.65960/girj.1.1.2025.6
32. Al Azhari, F. U., Shah, S. H. M., Al Azhari, S. I., Rasool, F., Ahmed, R., Samad, A., & Rehman, A. (2025). The role of Islamic economic principles in family law: A study on inheritance and property rights within the context of child protection. *Global Islamic Research Journal*, *1*(1), 59–76. https://doi.org/10.65960/girj.1.1.2025.2
33. Zubair, A. A., Salman, K., & Zakariyyah, A. O. (2026). Existing legal and regulatory framework for sovereign Sukuk in Nigeria. *Global Islamic Research Journal, 2*(1), 36–73. https://doi.org/10.65960/girj.2.1.2026.8
34. Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs*, *3*(5), 112–124. https://doi.org/10.71317/rjsa.003.05.0375
35. Abood, T. A., Dakhil, M. H., Nasef, A. J., Abed, A. Q., & Hamid, A. K. (2026). Authority and interpretation in Qur'anic studies: Re-examining classical tafsīr in contemporary Islamic scholarship. *Global Islamic Research Journal, 2*(1), 1–17. https://doi.org/10.65960/girj.2.1.2026.10
36. Alwan, F. Y., & Lilo, I. Y. (2026). Defending religious tradition in modern times: Comparative responses of Muslim and Christian scholars to scriptural criticism. *Global Islamic Research Journal, 2*(1), 18–35. https://doi.org/10.65960/girj.2.1.2026.11
37. Cami, G. (2024). Legal standards for cross-border access to electronic evidence in criminal procedure: An Albanian perspective on international standards. *Studia Iuridica Lublinensia*, *33*(5), 11–30. https://doi.org/10.17951/sil.2024.33.5.11-30