

## USE OF ARTICLE 164 QANUN-E-SHAHADAT ORDER, 1984 IN CRIMINAL JUSTICE SYSTEM OF PAKISTAN

**\*Kashif Masood Siddiqui,**

Department of Law, Dadabhoy Institute of Higher Education, Pakistan

([aimmstrading@gmail.com](mailto:aimmstrading@gmail.com))

**\*\*Dr. Tansif Ur Rehman,**

Teaching Associate, Department of Sociology, University of Karachi, Pakistan; and Visiting Faculty, Department of Law, Dadabhoy Institute of Higher Education, Pakistan

([tansif@live.com](mailto:tansif@live.com)) (<https://orcid.org/0000-0002-5454-2150>)

### Abstract

*The use of digital technologies and electronic evidence has now become an important part of criminal justice system of Pakistan, in the context of Pakistan's cybercrime, terrorism, financial fraud, communication crimes in electronic communication, and technology-related harm. This was a major advancement for the courts in admitting evidence generated through the use of modern equipment as compared to the traditional rules of evidence that emphasized oral and physical evidence in Article 164 of the Qanun-e-Shahadat Order 1984. While the provision outlines the enabling framework, there are numerous practical challenges in terms of reliability and admissibility to consider, such as authenticity, chain of custody, forensic analysis, and understanding of the judiciary system of the evolving digital technologies. In this paper, the focus is on some aspects of the interpretation, drafting, and implementation of Article 164 in the Pakistani legal system and on the case law and comparative practice, which will help identify the institutional barriers and process deficiencies. It means that digital evidence must be more precisely statutory, and have strong technical capacity, it must be specifically trained, and it must be standardized forensic practice, to achieve the evidentiary integrity, due-process rights, and fair and transparent administration of justice.*

**Keywords:** challenges, historical context, laws, opportunities, theoretical context

### Introduction

The digital technologies have already entered nearly any aspect of the contemporary world, and an increasing quantity of electronic information is available as a source of information in criminal cases (Tahir et al., 2025). This change has made jurisdictions such as Pakistan rethink the conventional evidentiary practices in the light of computer, smartphone, social-media, and surveillance-generated data. Electronic data, such as communication records and financial transactions, have turned out to be crucial in enabling investigators to combat online harassment, identity theft, and cyber fraud (Gul et al., 2025). In the meantime, digital evidence has certain issues of admissibility and confirmation since, in many cases, the courts lack the technical expertise to establish authenticity and integrity. Researchers therefore suggest the restructuring of the criminal justice procedures in such a way that they can handle electronic evidence in the same and trustworthy way (Nazir et al., 2025).

Though Pakistan has attempted to introduce a digital evidence provision as a supplement to Article 164 of the Qanun-e-Shahadat Order 1984, the provision is not a much-needed provision since it lacks a lot of guidance on the procedure requirements, like chain-of-custody, expert witness, and forensic verification (Neik et al., 2025). Courts do not suit well to consider electronic evidence because they are not technically trained and homogenous on the



quality of evidence. The relative analyses reveal that the standardized procedures of forensic practice, metadata retention, and integration of modern technology are required to streamline the domestic practices to the international practices (Qazi & Marvi, 2023). The absence of such reforms means that there is a chance of inconsistency in the application of digital evidence, which may jeopardize the principle of fairness and efficiency as far as the prosecution of crimes with the help of cyber-enabled methods is concerned.

### **Research Justification**

This study is essential because of the active growth of digital technologies in the criminal justice system of Pakistan. Electronic records such as CCTV footage, call-detail records, emails and social-media communications, computer logs, and forensic data of digital devices have become key in investigating and prosecuting crimes as varied as cybercrime and financial fraud to terrorism and internet-based harassment. The Qanun-e-Shahadat Order 1984 (Article 164) is the main law that governs the use of digital evidence. However, it does not provide any rules or standards for how to make sure that digital evidence is consistent and reliable. This provides the courts and investigators a lot of freedom but not much guidance. For this reason, the procedure has not been uniform, judges have lacked uniform interpretation, and there has been a lack of technical expertise. The justice system is open to the risk of innocent people being convicted, conflicts over evidence, delays in the process, and errors in investigations.

Additionally, cybercrime and other tech-assisted crimes have been on the rise, with increased frequency, the ability of the police, prosecutors and courts to identify, secure and properly preserve evidence, the interpretation of electronic evidence has come into great importance in the administration of justice, and it is effective and fair. The study paper can help the decision makers to address the gaps identified in the study, the legal frameworks, as well as determine the institutional capacity, and offer recommendations on the grounds of comparative practices. Ultimately, it would like to enable the criminal justice system to become more consistent, aware of rights, and use digital evidence in a clear and reliable manner.

### **Literature Review**

The policy and academic literature on digital evidence in Pakistan demonstrates the increasing gap between the legal framework and the realities of operation. The researchers add that although digital evidence is legally admissible as per such laws as the Qanun-e-Shahadat Order 1984 and PECA 2016, the authenticity, chain-of-custody, and technical integrity are often problematic, and the impact of uneven outcomes in the courts (Qazi & Marvi, 2023). The researchers also note that a lack of a well-defined procedure can also mean that judges can resort to ad hoc means or discretion, which can weaken the validity of electronic evidence (Gul et al., 2025).

The other central theme in the literature is that of the institutional capability and forensic infrastructure in regard to digital evidence. Many forensic labs around the world are found to be under-resourced, and uniformity in collecting, preserving, and examining electronic evidence is often lacking (Mahmood et al., 2024). The research of the law enforcement agencies and of the prosecutors shows that it is time to have personnel trained with the latest digital forensic techniques, proper tools, and working frameworks, which would ensure the integrity of the chain of custody (Chen et al., 2023). Past practices in the international community have revealed that reliable and admissible digital evidence can be significantly



improved with the help of organized forensic procedures, accredited forensic laboratories, and efficient technical methodologies (Ismail & Ariffin, 2025).

Moreover, the literature suggests that new technologies may improve the reliability and quality of digital evidence, for example blockchain-based systems that are proposed to provide an audit trail of how digital evidence is handled and stored, which would make criminal trials more transparent and reliable (Stoykova, 2023). The literature also stresses on the need to use open-source forensic tools, as proposed by experimental studies, to improve the admissibility of electronically obtained evidence (Atlam et al., 2024). A combination of these studies gives rise to the notion that the criminal justice system of Pakistan could be made better through both legal reform and institutional reinforcement, and by adopting the latest forensic technologies to ensure that the digital evidence is reliable, verifiable, and admissible every time (Kumar et al., 2025).

### **Historical Context of the Use of Article 164 Qanun-e-Shahadat Order, 1984 in Criminal Justice System of Pakistan**

The evolution of the law of digital evidence in Pakistan is historical because the evidentiary norms in the world, which were enhanced by the rapid technological change, were propagated. The traditional rules of evidence were reflected in the Qanun-e-Shahadat Order 1984 (QSO), which made oral testimony, eyewitnesses, and hard-copy physical evidence the most reliable evidence. Yet, this organization had served for quite a long time in the primarily analogue world. However, with the rise of computers, cell phones, and online communication, courts were forced to consider the emergence of new evidence that did not necessarily fall into the old categories (Nazir et al., 2025). This prompts policymakers and legal professionals to understand that the conventional rules were at a certain limit (Gul et al., 2025), and the empirical evidence demonstrates that judges do not necessarily possess conventional methods to examine authenticity and reliability (Haque et al., 2023).

Article 164 of the QSO was in response construed as a legislative attempt of the day to leave the question of admissibility of evidence generated by modern devices to the discretion of the courts. The initial step in the recognition of digital evidence as an important part of criminal prosecutions was the introduction of legislation such as the Prevention of Electronic Crimes Act 2016. Nevertheless, it is characterized by a shortage of appropriate laboratories, as well as workers who can provide the work on challenging digital cases (Parveen & Haider, 2024).

Comparative studies also contribute to the fact that the best practices on the international level, the standardized forensic working process, and metadata conservation are largely not provided in the current system of Pakistan. As a result, judges tend to be skeptical of digital evidence, which is based on ad hoc rulings or corroborative evidence, but not on procedural precedent.

### **Theoretical Context of the Use of Article 164 Qanun-e-Shahadat Order, 1984 in Criminal Justice System of Pakistan**

The law of digital evidence is informed by the basic principles of authenticity, reliability, and procedural fairness, which inform courts to evaluate the safe use of electronic data in adjudication. Unlike traditional types of evidence that may possess some inherent physical characteristics that lead to their credibility, digital information is non-material, and it is highly manipulable, replicable, or can even be destroyed accidentally. This vulnerability



creates a need for verification of the admissibility of the law. Evidentiary integrity theories place a high priority on the need for a chain of custody that allows for the tracking and transparency of the process from data collection through storage, transfer and processing to presentation at trial, and the assurance that the electronic record is not tampered with from the time it is collected until it is presented in court.

Another approach that has had a significant impact on the law of digital evidence is legal positivism, which suggests that the law must be clear and that judges, under this doctrine, have the authority to interpret the law. Due to the rapid change of technologies, this view puts emphasis on the need for the neutrality of technologies that allow courts to have sufficient discretion to change without affecting legal certainty. Socio-legal approach Technological determinism: Technologies change the way law is practiced, and courts must adapt historic doctrines used in a world without technology.

However, the procedural justice theory emphasizes the importance of fairness, equal treatment, and protection of privacy rights to prevent digital evidence that may be particularly damaging to innocence or guilt, such as surveillance data or device extractions. These theories provide clarity in the interpretation and application of Article 164 in the Pakistani legal system to effectively manage digital evidence in a responsible, and transparent way that will not undermine the constitutional rights.

#### **Laws Regarding the Use of Article 164 Qanun-e-Shahadat Order, 1984 in Criminal Justice System of Pakistan**

The Qanun-e-Shahadat Order 1984, under Article 164, authorizes the Pakistani courts to accept electronic evidence, it is a major breakthrough compared to the traditional theories of evidence, where we have to rely on oral evidence and physical documents. This provision leaves much at the discretion of the judges since they can decide on the relevancy, authenticity, and probative value of digital evidence on a case by case basis. Article 164, however, does not identify any procedural requirements (e.g., authentication standards, expert qualification, chain-of-custody requirements, forensic validation procedures), and courts have no standardized guidance to rely on when it comes to establishing reliability and legal compliance. In Pakistan there are number of laws that work along with Article 164 by recognizing electronic records and creating a system to collect and check their authenticity:

1. **Electronic Transactions Ordinance 2002** – Recognizes electronic records and digital signatures, establishing principles for authentication and recognition of electronic documents.
2. **Prevention of Electronic Crimes Act (PECA) 2016** -Includes cybercrimes, legalizes electronic collection of evidence, maintains records by service providers, as well as the illegalization of alteration of electronic records.
3. **Pakistan Penal Code (PPC)** - Includes the provisions on interference with evidence, hindering justice, fraud, and other related crimes of digital evidence integrity.
4. **Code of Criminal Procedure (CrPC) 1898** - Governs the procedural character of criminal trials, comprising the gathering, display, and admissibility of proof that is expanded to digital proof.

#### **Challenges for the Use of Article 164 Qanun-e-Shahadat Order, 1984 in Criminal Justice System of Pakistan**

There are a number of issues that challenges the admissibility of digital evidence in Pakistan, which effects the accuracy, impartiality, and efficiency of criminal justice procedures. First, the issue of authenticity takes precedence since any digital data is prone to editing, erasing, or forging. Emails, call-detail records, CCTV footage, and computer logs are easily manipulated without leaving behind any traces, and thus difficult to verify. Without standardized chain-of-custody procedures, courts have difficulty determining whether digital evidence has been preserved between seizure and analysis to courtroom presentation, and the validity of that probative value is compromised.

Second, there is a huge shortage of forensic laboratories in Pakistan. Current cybercrime and digital-forensic services have small staff levels, a lack of current technology, and a large case backlog, which makes the forensic reports less credible. Numerous laboratories are not accredited or do not have standard operating procedures and it becomes hard to achieve international evidentiary standards. Third, investigative agencies lack adequate expert training in how to appropriately seize, maintain, and deal with electronic evidence. Unprofessional practices like not isolating devices off networks or not performing an adequate process in imaging put the risk of contaminating data and undermine prosecution cases.

Fourth, the technical skills of the judicial officers are mostly lacking, and therefore, often there is a lack of uniformity in the ruling, giving it a more personal than forensic character. This lack of consistency contributes to a lack of predictability in the law, as well as the possibility for procedural miscarriage or unfairness. Fifth, there is a lack of coordination between the police, prosecutors, and forensic laboratories that delays the investigation process, makes it difficult to verify the results, and leaves accountability unclear.

At present, no data-protection laws are enforced in Pakistan, and this ambiguity about the boundaries of investigative powers and the privacy of citizens. All of these problems show that the criminal justice system needs to be changed. For example, there should be a standard of forensic procedures, technical training, more judges, and better data protection. These changes will make digital evidence more reliable, fair, and useful.

### **Opportunities for the Use of Article 164 Qanun-e-Shahadat Order, 1984 in Criminal Justice System of Pakistan**

Despite the challenges associated with digital evidence, it offers great help to empower the criminal justice system, in addition to modernizing the investigation and prosecution systems in Pakistan. Firstly, electronic evidence can significantly enhance the quality of investigations. CCTV footage, mobile-phone records, GPS tracking data, call-detail records, emails, and digital financial transactions are some of the data that can provide objective data that can either corroborate or disapprove witness testimony. With a source of verifiable facts, this kind of evidence can eliminate the use of oral testimony, which can be prone to memory lapse, bias, or coercion, and enhance the credibility of judicial decisions and reduce cases of wrongful conviction.

Second, the use of electronic evidence improves accountability and transparency in law enforcement. Body-worn cameras, massive digital records make it a disinterested record of police activity, compliance with rules, and investigation steps. These mechanisms are capable of not only assisting in identifying and preventing misconduct but also establishing trust in the justice system by showing that the actions are recorded and can be proven.



Third, superior digital-forensic tools enable the authorities to explore sophisticated crimes in a better manner. Both online fraud, cybercrime, harassing people, and breaches of data can be monitored and analyzed with the aid of forensic software, which enables investigators to more firmly associate perpetrators with crimes and to pursue previously unreachable or difficult to prosecute crimes. Fourth, electronic systems enhance the effectiveness of case management. The coordination among the police, prosecutors, and courts is achieved through electronic filing systems, online centralized e-crime portals, and automated record-keeping systems. Quick access to evidences, reduce the time spent in paper work, and improving the management of records can accelerate the trial process to clear the case backlog and improve the overall system responsiveness.

Fifth, digital evidence supports international cooperation in the investigation of crimes. With increasing cases of transnational crimes, cybercrimes, the ability to share forensic evidence, cross-border investigations, and the ability to collaborate with other foreign agencies is critical to successful prosecution and coordination of law enforcement. Overall, when managed and assisted by standardized procedures and accredited labs, and judicial education, digital evidence portrays a groundbreaking chance to the criminal justice system in Pakistan, despite improving accuracy, effectiveness, accountability, and the ability to effectively combat contemporary crime

### **Discussion**

As the Article 164 analysis shows, Pakistan has already achieved some significant steps towards incorporating digital evidence into its criminal justice system, but there are still considerable gaps in the actual application. The clause provides courts the authority to admit electronic records, but there has been little guidance on the process, and this has led to inconsistent judicial rulings and treatment of electronic records from state to state. The judge and forensic investigator lack technical training, and there are no uniform forensic guidelines; these also impact the reliability and admissibility of digital evidence.

The courts are acknowledging the advantages of electronic recordkeeping, but the various treatment and authentication of the records could lead to unfair and unreliable results. The value of digital evidence in investigations and prosecutions is acknowledged, notwithstanding these challenges. In the future, some reforms are needed to bring balance between the judge's discretion and the formality of proceedings. For uniformity, it is important to have detailed legal guidance and to be accredited. A forensic laboratory and training of judges and law enforcement officials. Effective management of digital evidence will depend on the implementation of privacy protection measures, inter-institutional collaboration, and international best practices, as well as other factors that contribute to success demonstrated by experiences in other countries. Such reinforcement of digital evidence is provided by the digital context, will be able to become a responsive, responsible, and rights-respecting process that will improve the reliability and effectiveness of the criminal justice system, without harming the rights of individuals.

### **Conclusion**

The Criminal justice system in Pakistan must incorporate Digital evidence that can help the investigation, witnesses' testimony, and make the prosecutor's job easier. Despite the provisions of the Qanun-e-Shahadat Order 1984 permitting the use of electronic evidence in the court, the same has not been done yet, due to prosecutorial authority and the absence of a



clear judicial framework. Clear judicial rules and a limited prosecutorial role, combined with unclear procedural rules, severely restrict the potential of this provision, and uneven interpretations of the law by judges are also a threat to the reliability of the judicial system.

The use of digital evidence can bring change in the criminal justice system of Pakistan, but only when a complete change occurs. Standardized chain of evidence, more investigators, and credible forensic laboratories, more experts to assess and evaluate, and the assessment of the crime will be more accurate and efficient, with digital evidence. Coordination between police and other relevant agencies is also very important. The process of modernization of the evidentiary system can be seen not merely as a technological or administrative requirement but also as a fundamental requirement for demonstrating citizens' trust, accuracy, and fairness within the criminal justice system in the long run.

### **Recommendations**

First, the system of digital evidence and its utilization in the Pakistani courts should be streamlined and established with clear requirements with regard to authentication, qualifications of experts, and standardized procedure in forensic handling of evidence that would provide the courts with a clear and definite conception of admissibility. Concurrently, national digital-forensic standards should be set that are uniform, reliable, and trustworthy in the management of electronic records based on international best practices. To facilitate proper evidence analysis, it is necessary to create accredited forensic laboratories with modern technology and staffed by qualified specialists, and introduce chain-of-custody practices that would be required of all digital materials to maintain integrity between the collection and presentation in a courtroom.

Investment in human capital is also important. Digital evidence and forensic procedures, as well as methods of cybercrime investigation, should be specially trained for judges, prosecutors, and investigators. Cybercrime modules and legal-technology courses may be introduced into police academies and law schools to build knowledge in the early stages. To enhance research collaborations between law enforcement and forensics teams, a centralized digital-evidence management system will be implemented to improve coordination, record-keeping, and accessibility during an investigation, and the joint investigation teams and inter-agency procedures may be improved to tighten collaboration.

Moreover, a data-protection law should be passed in the country that is as comprehensive as possible in order to protect the right to privacy as well as control lawful access to online data. Cross-border sharing of evidence should be encouraged at the international level so that cybercrime and financial fraud cases can be solved. Education and sensitization of the citizens on the legal aspects of digital use will result in a culture of obedience and prevent the abuse of technology. All these measures taken together can establish a strong, open, and trustworthy system to handle digital evidence, so that Article 164 could be a powerful tool of justice without infringing individual rights.

### **Research Limitations**

The secondary literature, judicial comments, and policy reports are available, making for an important source of information, but it is not necessarily reflective of the actual experience of the implementation of Article 164 under the Pakistan criminal justice system, which is in question and is being implemented in practice. The data regarding digital-forensic capabilities, lab certification, and there is still limited investigation of the investigative

procedures, and they are not capable of acquiring a comprehensive understanding of institutions. The information on digital-forensic capabilities, laboratory certification, and investigative procedures is still limited, and it is not possible to get a deep knowledge of the institutions.

The study's conclusions are further complicated by the dynamism of the technological evolution; the new tools, software and cybercrime methods may soon make old practices or interpretations of the law irrelevant. In addition, Pakistan is a federation and the opportunity exists to differ the implementation of the national law in the provinces, thereby adding further complications that are not always found in the literature. The study cannot make any judgment about operational issues, procedural delays, or resource issues faced by judges, prosecutors, and forensic investigators in the field because it did not include primary data collection, which is defined as conducting interviews or field observations. All these factors indicate that although the study gives a good theoretical and legal background, the results should be taken with a grain of salt, as there are chances that the formal and practical application of the law may differ.

### **Research Implications**

The present research paper provides a critical foundation for policymakers, practitioners, and researchers working towards the modernization of Pakistan's evidentiary system particularly in relation to the introduction of Article 164 in relation to digital evidence. The results offer practical guidance for legislative reforms and the formulation of special training, as well as effective and efficient application of technical and human resources for the judiciary, by analyzing the gaps in judicial interpretation, forensic capacity, procedural standards, and inter-agency coordination.

To legal scholars, the study highlights the need to incorporate the doctrinal analysis with technological factors to make sure that the evidentiary law keeps up with the current digital realities. To the justice sector, the study points out feasible measures of improving court preparedness, such as instituting standard procedures, accreditation of forensic labs, and special judicial and investigative education. Furthermore, the study will have implications on the global best practices and collaborative models that can help strengthen the credibility, effectiveness, and equity of criminal investigations involving digital evidence, thereby boosting the public trust in the judiciary system of Pakistan.

### **Future Research Directions**

The empirical analysis of the processing of digital evidence in real cases should be prioritized for future research to understand how the procedure, resource allocation, and interpretation of the digital evidence would be challenged with regard to Article 164. There is a need for comparative analysis of the forensic labs and cybercrime etc units in South Asian countries. Identify models and best practices that can be scaled up and adapted to the context of Pakistan, its legality, and institutional structure. Studies that have explored public attitudes towards digital privacy, surveillance, and security would also contribute to issues of social and cultural concerns that would benefit the community, impact the authenticity and legitimacy of digital evidence.

Besides this, there's a critical need for interdisciplinary discussion between the Law, Computer Science, and Criminology. Peer Reviewing a forensic tool in a Courtroom for reliability, integrity, and admissibility. The development of judicial decisions, case law, and

processes of judicial decision-making will be tracked through longitudinal research. Procedural evolution would provide some analytical clarity to the development of legal standards. As digital evidence evolves, it is important to keep in mind that there are important considerations to take into account. All of this research can be used to improve the effectiveness of digital-evidence governance in Pakistan.

## References

- Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics*, 13(17), 3568. <https://doi.org/10.3390/electronics13173568>
- Chen, C., & Dong, B. (2023). Digital forensics analysis based on cybercrime and the study of the rule of law in space governance. *Open Computer Science*, 13(1), Article 20220266. <https://doi.org/10.1515/comp-2022-0266>
- 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>
- Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: An analysis of the cyber threat landscape and readiness. *IEEE Access*, 11, 40049–40063. <https://doi.org/10.1109/access.2023.3268529>
- Ismail, I., & Ariffin, K. A. Z. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLOS ONE*, 20(9), e0331683. <https://doi.org/10.1371/journal.pone.0331683>
- Kumar, G., Saha, R., & Conti, M. (2025). ZAKON: A decentralized framework for digital forensic admissibility and justification. *Information Processing & Management*, 62(6), 104226. <https://doi.org/10.1016/j.ipm.2025.104226>
- Mahmood, H., Arshad, M., Ahmed, I., Fatima, S., & Rehman, H. U. (2024). Comparative study of IoT forensic frameworks. (2024). *Forensic Science International: Digital Investigation*, 49, 301748. <https://doi.org/10.1016/j.fsidi.2024.301748>
- Nazir, S., Asif, M., & Khan, A. U. A. (2025). Digital evidence in Pakistan: A doctrinal assessment of admissibility and reliability in criminal trials. *Advance Social Science Archive Journal*, 4(1), 1941–1951. <https://doi.org/10.55966/assaj.2025.4.1.0107>
- Neik, S., Azhar, S., & Niazi, A. (2025). Forensic evidence under domestic law: An efficient substitute to ocular account in Pakistani courts. *ACADEMIA International Journal for Social Sciences*, 4(2), 467–474. <https://doi.org/10.63056/ACAD.004.02.0190>
- Parveen, K., & Haider, G. (2024). Digital investigations: Navigating challenges in tool selection for operating system forensics. *International Journal for Electronic Crime Investigation*, 8(1), 79–92. <https://doi.org/10.54692/ijeci.2024.0801189>
- Qazi, M., & Marvi, M. (2023). Infusing digital technology in judicial operations in Pakistan: A critical analysis of global best practices and local initiatives. *SSRN*. <https://doi.org/10.2139/ssrn.4378378>



- Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law and Security Review*, 49, Article 105801. <https://doi.org/10.1016/j.clsr.2023.105801>
- Tahir, M. I., Saeed, A., Murtaza, M., & Abdullah, H. O. (2025). The impact of artificial intelligence on evidence in criminal trials. *Social Science Review Archives*, 3(3), 1882–1894. <https://doi.org/10.70670/sra.v3i3.1023>