Journal of Social Sciences Review (JSSR) DOI: https://doi.org/10.54183/jssr.v3i1.198

How to Cite This Article: Khan, M. S., & Bhatti, S. H. (2023). Digital Evidence and Pakistani Criminal Justice System: A Review Article. *Journal of Social Sciences Review*, 3(1), 489-498. https://doi.org/10.54183/jssr.v3i1.198

Digital Evidence and Pakistani Criminal Justice System: A Review Article

Muhammad Sajid Khan	Ph.D. Law Scholar, Times Institute, Multan, Punjab, Pakistan.
Shaukat Hussain Bhatti	Assistant Professor, Times Institute, Times Institute, Multan, Punjab, Pakistan.

Vol. 3, **No.** 1 (Winter 2023)

Pages: 489 – 498

ISSN (Print): 2789-441X

ISSN (Online): 2789-4428

Key Words

Digital Evidence, Pakistani Criminal Justice System, Supreme Court, Legislation, Law

Corresponding Author:

Muhammad Sajid Khan

Email: pathancj131@gmail.com

Abstract: *The value of digital evidence has expanded quickly in recent years due to increases in its dependability and complexity. Evident from national and international regulations. There is a presumption in the law that digital evidence is admissible, and authorities have been directed not to rule it out of court because it is not presented in a substantive and perceptible form. Domestic and international laws have educated domestic law, and today everyone agrees. This section examines the background of the issue, the laws at play, and how it presented the matter to the Supreme Court nationwide. The technique adopted in this review study is a literature search. "Digital evidence" refers to any evidence made, kept, or transferred via digital means. It is impossible to overstate the role that digital evidence plays in the administration of criminal justice. In Pakistan, there were no laws surrounding the acceptance of digital evidence in court until 2002. We review roughly twenty evaluations given by different scholars in their articles. Part one of this review article's subsections is split in two. These abstracts expand upon the newest parts of the supplied legislation. The last section often supplies a quick summary of the important points and supporting evidence presented throughout the essay.*

Introduction

A functioning criminal justice system is crucial to sustaining the rule of law. It is so because the Rule of Law guarantees that everyone is treated equitably under the law by providing a basis for civil liberties, legal protections, and accountability mechanisms. Due to the expansion of contemporary technologies and the increasing complexity of cases, the criminal justice system in Pakistan needs reform in some areas. To fill in the cracks in the current criminal justice system, it should amend the criminal law to match the demands of time and the necessities of society. Nonetheless, given the quick rate at which digitalization is penetrating all sectors of society, there is a pressing need for changes in the administration of digital evidence so that cases can be treated more swiftly and efficiently. In light of the ubiquitous availability of digital devices and information, however, legislatures and courts have realized the relevance of digital evidence, leading to the promulgation of the Electronic Transaction Ordinance, 2002 (ETO) and revisions to existing legislation. However, digital evidence requires verification with other tangible evidence and is not accepted as primary evidence in a court of law. The courts in Pakistan have historically placed little weight on digital evidence.

The decree made significant revisions to the established evidence rules in civil and criminal cases. The ordinance fundamentally recognized digital or electronic evidence's supremacy over physical evidence. Electronic documents, information, records, and transactions have their validity proven, putting an end to the urban fallacy that data saved or transferred digitally is

no more dependable than information kept in paper form. Although ETO 2002's deployment has substantially enhanced the digital evidence environment, it is crucial to emphasize that there are still certain grey areas.

Nonetheless, the evidence has been designated as primary and can meet the best evidence test's threshold for admissibility. However, various observations made by judges of Pakistan's superior courts show that its appreciation or weight is still left to the court's discretion. The ordinance essentially treated digital or electronic evidence as primary. It also established the veracity of data recorded or transferred digitally, putting an end to the popular idea that such material is no more dependable than hearsay. Two, the law underlined that digital evidence could be adequate to meet the Best evidence criteria. The Electronic Transactions Act of 2002 is another piece of legislation that underlines the value of digital evidence. The research indicates that article 164 QSO is more permissive than an obligatory provision and leaves more to be wanted in specifying what constitutes a current device, but that the adoption of ETO 2002 is helpful in the sense that it has clarified the position of digital evidence. Due to the ETO 2002's clarifications, digital evidence is now primary and can pass the best evidence standard if necessary, although the court still has discretion over how much weight to give it. It is because a few judges on Pakistan's highest courts have aired their thoughts on the matter. As a result of these considerations, the evidence has been classified as primary and meets the criteria for the best evidence test. Therefore, it may be somewhat accurate to state that digital evidence is still corroboratory concerning the weight of the evidence. There is a difference between computer-stored and computer-generated evidence when considering major evidence. Computer-generated evidence, such as transaction receipts, looks to pass the originality test. It is hard to fabricate further copies after the first one is created, as required by the ETO 2002. This is because the ETO 2002 only considers evidence to be primary if it is the original and has not been modified in any way except for natural additions or decay. However, it is prudent to consider any evidence in a computer, as it may readily be edited or added to. In other words, it adds validity to our thesis and should be interpreted as such. To properly value electronic evidence, as opposed to merely admitting it, the review paper will argue that it must judge it against the tried and proven criteria stated in worldwide best practices. These are genuineness, dependability, a chain of custody, and trustworthiness. The review essay will argue that comparing electronic evidence to more traditional types of proof is crucial for thoroughly appreciating its usefulness.

Discussion

Digital devices are ubiquitous, and their use has increased dramatically across all fields. For instance, nowadays, everybody uses email or IM to talk to each other. Similar to how film has given way to digital photography. Digital signatures are used for both specifying the conditions of the contract in digital documents and acknowledging those terms. Nevertheless, there are significant differences between offline activities and their digital counterparts. After completing a digital activity, it is feasible to monitor its history and observe exactly what it performed actions along the way. For example, if you remove something from your computer's files, you can typically retrieve it back. Any time you delete something from a storage device, whether a hard disc, a flash drive, or a floppy disc, that information is no longer physically present on the device. Still, it may retrieve through an external storage engine or by contacting the system administrator. A digital device's history can be decoded and reconstructed for any acts done by the user. However, it is easy to disguise your tracks and destroy all traces of your wrongdoing if your

crime entailed the physical act of accomplishing anything. Because of this, the weight of digital evidence has expanded dramatically since the turn of the century. Since this is the case, it is time to specify what counts as digital proof.

According to JPA Yaqoob, in his article, advanced digital techniques explain that Digital evidence refers to data stored or transmitted in a binary format that may be admissible as proof in a court of law (Yaacoub et al., 2022). The National Institute of Justice has found this to be the case. It can be located on a computer's hard drive or a mobile device's storage medium. E-crime, sometimes known as cybercrime, is commonly related to digital evidence and might refer to things like child pornography or credit card fraud. However, digital evidence is being utilized to prosecute all crimes, not only e-crime. Once upon a time, this was not the situation. Evidence about suspects' motivations, whereabouts at the time of the crime, and links with other suspects may be located in their emails or the files on their mobile phones.

The Qanoon-e-shahadat order of 1984 and Computerized Evidence

In his 2022 paper titled "Digital evidence and the administration of criminal justice," Dr. Guffran Ahmed notes that Articles 59 and 164 of the Pakistani Constitution address digital evidence issues. This means that digital evidence can be collected using high-tech gadgets in Pakistani courts. According to Article 46-A o, digital evidence, as well as evidence manufactured or kept mechanically, is admissible.

The Qanoon e Shahadat order (1984), Article 46-A, and Article 78-A of the Qanoon-e-Shahadat order, and the Electronic Primary electronic papers are acceptable digital evidence under Article 73 of the As it is able to produce copies of previously saved data, it can assert that the article is about data generated by a computer and not data kept on one. Even if this is true, judicial interpretation remains essential due to a recent ruling by LHC Judge Mr. Shahid Kareem, who ruled that primary electronic documents will be treated as evidence and susceptible to cross-examination. Authenticity, dependability, and admissibility are characteristics that must be met for electronic evidence to be recognized globally. To avoid the loss or alteration of evidence and so meet these requirements, a chain of custody must be established. Simultaneously, it is collected, and the names of the first responders to the crime scene are recorded. Article 164 of the 1984 Qanoon-e-Shahadat ruling refers to the following: "Construction of evidence that has been accessible due to the use of current technologies; the court may accept any evidence created using modern equipment and technology if it deems it appropriate." "Easier evidence construction due to the prevalence of digital tools." In spite of regulatory and procedural impediments generated by the broad adoption of digital tools, a Modern article asserts that service and communication delivery was executed effectively. Due to the fact that the challenges of the manufacturers were not signed and unattested, they aroused suspicions about the execution, making these forms of communication challenging and insufficient for faith in the legal system. Due to the Electronic Transactions Ordinance, legal obstacles have been removed, despite the misunderstanding regarding unsigned proof of the makers via electronic devices.

Zaman and others Discussed in their article an overview of the criminal justice system about Article 2 of the 1984 order Qanoon-e-Shahadat was revised in 2002 to include the Electric Transactions Ordinance. The Electronic Transactions Ordinance is nevertheless applicable despite the ambiguity surrounding the unsigned electronic proof provided by the producers (Zaman & Bhatti, 2023).

According to Pakistan's Electronic Transactions and Digital Evidence Ordinance: An analysis of the article on digital evidence and the criminal justice system by The fundamental argument against digital evidence is not that we

need additional evidence to support it, such as a printout, but rather because it is not direct or first-hand information that is directly extracted from a device. With the passage of the Electronic Transactions Ordinance, The ETO was into effect in 2002. According to the revised ETO, digitally obtained information in the form of a document, transaction, communication, or audiovisual recording cannot be rejected only on the basis of its digital nature. This includes audio and video recordings as well as file transfers and verbal communications (Solanke & Biasiotti, 2022). Because such evidence is considered to be direct evidence, it is deemed relevant and admissible. Digital data is one piece of direct evidence that can be used to prove the existence of a particular occurrence. Before digital evidence is considered credible, it must be integrated with other types of evidence and external events and circumstances. Previously, the admission criteria for digital evidence were distinct

Article 5 of ETO was amended in 2002 to update these rules. Article 5 of the ETO specifies that if digital evidence is presented that has not been altered in any way, it shall be recognized as admissible proof, even if the alteration was performed inadvertently (Saeed & Gillani, 2021). All of these adaptations are being made to meet the needs of modern society, in which the great majority of transactions, including payments, are conducted digitally, and contracts are either approved or acknowledged as legally binding on all parties.

However, it cannot be stated that the advent of ETO and the other improvements provided by QSO have elevated digital evidence from the category of corroborative evidence to that of direct or original evidence. This is owing to the fact that ETO's transformations are not identical to QSO's. Since stored information can be utilized to produce more copies, one could argue that the article only relates to information created by the computer and not saved on it. Judge Mr. Shahid Kareem of the LHC has just ordered that electronic papers will be recognized as primary evidence susceptible to cross-examination. Therefore this interpretation would require judicial intervention. Similarly, it is obvious that documents created using electronic technology are admissible as primary evidence; it is reasonable to presume that the article refers to computer-generated data. In addition, some global conditions must be met for the admissibility of electronic evidence. This checklist includes items for originality, dependability, and acceptability. All of these objectives can only be accomplished if the evidence is not tampered with or lost between the time it is collected and the time it is submitted to the proper authorities.

The Pakistani Legal System Accepts the Following Modern Technologies as Admissible Evidence

Following the alteration and passage of various sections of Qanun-e-Shahadat 1984, court procedures in Pakistan are increasingly dominated by presenting evidence from contemporary gadgets. Following is a discussion of the different modern instruments used to depict the facts in Pakistan and references to instances that it settled with the aid of those tools.

Coverage in the media, including articles and videos: According to the Pakistani Supreme Court, a press report is admissible in the judicial system if it is written for the benefit of others rather than the reporter's interests and goals. The contents may provide the necessary evidence to demonstrate that they threaten the administration of justice. Two, using faxes as evidence in the legal system has facilitated the resolution of cases more promptly and efficiently. The District Court has been presented with a case (2019 PLD 602) involving a dispute over constructing a nightclub on Railway land. The initial fax forwarded by the railway administration to the proper respondent contained no hint of objection. After a while, it became a source of dispute. The court concluded

that sending a private fax to the respondent during private correspondence was improper since it breached the bidding rules. The advertisement should communicate the railway administration's norms and regulations to the general public. Therefore, the petitioner has prevailed in this case.

Thirdly, electronic communications and online connections have been valuable pieces of evidence in resolving criminal cases before Pakistani courts. A terrorism-related case was resolved using the Anti-Terrorism Act. The email was associated with threats of physical danger or kidnapping. Uncontestable evidence connected one of the co-defendants to the installation of a computer, internet service, and email account. The federal government fabricated a threat to public safety and security in response to pressure from an external party. Any internal factors did not influence this decision. After verification by the technological forensics team, the email cluster and the record of the source of the email sent over a particular internet connection were valuable in identifying the suspect. As a direct result, law enforcement authorities were able to locate technological devices used to communicate with the deceased. Utilizing technology such as a computer, scanner, Polaroid camera, and zoom camera, the deceased's loved ones could maintain contact and forge enduring bonds after their passing. After it revealed the truth, the accused and their co-defendants were apprehended, and the court ultimately sentenced them to life in prison.

According to the article, the mobile phone, often known as a cell phone, is a compact, portable electronic device that provides quick, long-distance communication in a personal setting. In addition to making and receiving phone calls, cell phones contain text messaging, SMS, email, internet access, MMS, and the capacity to produce and view images and videos. As a sign of satellite cell phones, smart cells are connected to the cellular network of base stations, which is connected to the Public Switch Telephone Network.

Evidence Acceptability and Weight

Although it is great that the ETO has been modified to reflect the rising acceptance of digital evidence, it is important to note that these modifications make no reference to the weight or value of such evidence. For digital evidence to be considered during the review process, the courts in Pakistan need to provide some guidance at this level. It goes to reason that only some components of the law in Pakistan, a country whose legal system is based on common law, would be codified into statute. In common law countries, citizens must be familiar with judicial precedents to comprehend statutory language's meaning fully. While ETO 2002 and later amendments to the QSO have clarified the primary status of digital evidence, the criteria under which it will be accorded weight remain still being determined. Since this is the case, clarifying how to make digital evidence admissible in court is vital.

Difficulties Associated with Digital Evidence

Because digital evidence is a form of physical evidence, it provides forensic analysts with unique issues. This form of evidence is especially challenging because it is filthy and slippery. · Only a portion of this jumble may be relevant to a given situation; therefore, it is essential to select the relevant information, make it relevant, and put it into an understandable format. · The information on a hard drive platter consists of a mishmash of bits and bytes that have become jumbled and layered over time. Second, digital evidence is frequently an abstraction of a digital object or event. As stated in a 2020 article by Venema and Farmer, when a person instructs a computer to do anything, like sending an email, the following events generate data trails that only provide a partial view of what occurred. Because we have the email and server logs, our knowledge of what occurred is restricted. In addition,

retrieving a lost file from a storage medium using a forensic tool involves multiple levels of abstraction. The magnetic fields of the disc serve as one layer, while the characters and numbers on the screen serve as another. Each abstraction layer can produce errors Carrier, 2021. This situation is comparable to how police normally investigate a crime scene. Similar to a jigsaw puzzle, homicide investigation clues can be fitted together to determine what occurred. It is impossible to reconstruct the crime entirely because not all the puzzle pieces are now available.

Murtuza Khan, The author of an article titled "Digital Evidences and Their Circumstances," argues that it is difficult to trace online behaviour to a single individual due to the circumstantial nature of digital evidence. Digital evidence can never substitute other types of evidence in a complete investigation. Digital evidence, such as time-and-date stamps on computer files, can be beneficial, but it cannot be the only evidence in a case. There needs to be more evidence to be collected from this source. Even if no evidence is offered, one could argue that someone else was using the computer at the time. Password systems protect some computers, but these can be broken, and many others do not require a password at all, making them open to anybody. Similarly, if the defense claimed that important pieces of exculpatory digital evidence were not collected from a specific system, this would only weaken a case without independent evidence of wrongdoing and already had limited strength. This would only be useful in an extremely dire situation.

A New Attitude toward Electronic Evidence

According to the PSSR article, DR.Hammed does not exist. 2021 Even while the interpretation of electronic evidence in Pakistani law has generally been well-received, it has recently been questioned in cases such as Rehana Anjum v. ASJ, etc. As a side note, it is important to note that Mr. Shahid Kareem, Judge of the LHC, who recently decided that electronic documents will be accepted as primary evidence and will be subject to cross-examination, was the author of the ETO 2000 amendments that were discussed and disputed. In addition, electronic evidence must adhere to certain rules to be admissible in court, which necessitates a chain of custody to prevent data tampering or loss. The entire first response team is included in this chain of custody. In 2021 the Supreme Court of Pakistan ruled that video evidence is acceptable in court under the following conditions: the origin of the evidence must be proven, and the judge must be able to explain how the evidence is assimilated. Second, a forensic report declaring that the video has not been tampered with should be provided to the court as proof that the footage on display has not been altered. The video evidence will only be admissible in court if these conditions are met.

In the current case, 2019, technological forensics verification and testing are necessary before an audio or video recording may be produced in court as admissible evidence. According to Article 164 of the Punjab Forensic Science Agency Act, which was reviewed for this article, this is the case. This must be accomplished before presenting the recording to a legal body. All of the alterations to QSO necessitated by ETO 2002 are centered on the admissibility of evidence rather than its significance (Bartels, 2022). Given the modifications' emphasis on computer-generated proof, this argument is bolstered. QSO and ETO have made it plain that digital evidence may be presented in court, but the court will still require physical corroboration before accepting the evidence. Evidently, in Pakistani courts, the probative value of digital evidence has begun to take precedence over its basic admissibility. The ETO 2002 modifications to QSO deal solely with admissibility; they say nothing regarding the weight or relevance of the evidence (Bartels, 2022).

According to the article, expert evidence in the justice system of Pakistan has value if

requirements incorporated in PLD 2019 SC 675 are fulfilled in accordance with the laws governing the presentation of evidence. When a video or audio recording was offered as evidence, the court nonetheless required verification of its legitimacy. It was vital to show evidence of the recording's accuracy in order to deny the likelihood that it had been altered in any way (Rasool & Rasool, 2022). To be admissible as evidence, the audio or video recording must be an authentic document of the conversation or incident as it occurred at the time it was made, or as it occurred at the time it was made (Rasool & Rasool, 2022).

According to the article Producing the individual who recorded the conversation or event, as well as their own audio or video recording of the exchange, was required (Solanke & Biasiotti, 2022).

In this instance, JDSS was produced by the admissibility of digital evidence specified in Pakistan's fundamental law. Digital evidence is acceptable under all applicable laws and can be utilized to establish a precedent and influence the legal systems of other nations in a manner that inspires respect. The admissibility of digital evidence is specified in Pakistan's fundamental law.

The investigation is the most important step in any procedure. The higher the precision and breadth of the investigation, the greater the probability that the guilty will be brought to justice and laws will be reevaluated in light of emerging dangers. A court may freely rely on an investigator's investigation when considering a case if it is convinced that the investigation is factual, impartial, and unbiased. When the investigation is not conducted honestly, the defence attorneys raise legitimate doubts about the evidence, and the court gives the accused the benefit of the doubt and acquits them.

• Experts play an important role in both traditional and digital investigations. For instance, the criminal procedure of the United Kingdom improved the expert opinion by permitting its use as an appropriate aid to the court. An expert witness must provide advice objectively, depending on his or her knowledge and experience, when requested by the court. Whenever the court requests an expert's opinion, the expert must provide one (Hameed, 2021). Only a court or the institution from which he receives paid might provide such instructions. Experts assist the court by utilizing their knowledge and abilities; they are not investigators, and their role is to assist the court whenever it requires the competence of an expert on a topic related to their profession. As was made plainly clear above, the expert's evidence in court carries the utmost weight. An expert is a person who offers the court helpful information by applying their experience. Cyber theft and robbery are significantly more serious than other types of crime (Hameed, 2021).

The current legal framework governing cybercrime and digital investigation can be determined by comparing the legislation of the last decade with those of the present. Cybercrime affects the entire world. The remaining nations have each provided their interpretations of the criteria, but none have declared theirs to be the definitive version. This is because none of the standards provides a haven for cybercriminals. When deciding whether to grant post-arrest bail in a case involving the Prevention of Electronic Crime Act, 2016 (for which an FIR had been filed), the Lahore High Court deferred to the investigative authority's report containing digital evidence instead of using its discretionUsman bin Farooq v. State 2018. The news of the tragedy quickly circulated. IT professionals assist detectives in locating and connecting the claims by analyzing the suspect's mobile phone records and Internet Protocol IP address. This is an essential aspect of the investigation. Collaborative analysis of digital evidence presented to the court is presented in a second key judgment.

- According to the article reviews by Majeed, The rules governing the acceptance of digital evidence have not kept pace with the rapid evolution of legislation in other nations. In addition, the primary source of evidentiary law in Pakistan is the Qanun-e-Shahadat Order from 1984, which was modeled after the Evidence Act of 1870 (Majeed & Hilal, 2022).
- This statute, which the British Empire enforced on the Indo-Pak peninsula, lacks the essential Sharia standards about proof and witness Abbasi, Rafique, and Badshah. This evidence must have an additional layer of verification that is not required anywhere else. Providing legally valid evidence requires digital forensic analysis, which involves additional security considerations (Lewulis, 2021). The year 2020 was mentioned in his article by Abbasi & Iqbal 2020.
- Usman demonstrates in his article that cybercrime has increased due to the usage of current technologies. As a result of the construction of a National Response Centre for cybercrime, the Federal Investigation Agency (FIA) will have the resources necessary to stop online misbehaviour and present current evidence to the judicial system to resolve cases. The department strives to better equip law enforcement agencies in the fields of information system security audits, digital forensics, penetration testing/training, and technical investigation (Usman, 2017).
- In addition, as described in the article by Zakar, Zakar, Qureshi, and Fisher (2014), the improper use of modern technologies is contributing to an increase in the number of crimes and the accumulation of more current evidence as a direct result of illiteracy counts more for participation in criminal activity, particularly among women in rural areas.

Conclusion

After assessing the merits and cons, it is considered that technological evidence presentation aids have entered and improved the legal system. The manner in which Article was revised to integrate ETO 2002 and the amendments made by QSO 1984 is indicative of its evolution. The purpose of these changes is to bring digital evidence closer to what is known as "primary evidence." Article permits the admissibility of evidence made possible by contemporary technologies. However, the court has the power to decide whether such evidence should be admitted or excluded. Therefore, courts view such documents as secondary evidence that requires independent verification. Since the law changed, it is no longer admissible as hearsay. Despite the fact that the admissibility of such evidence has been established since before ETO 2002 went into force, recent judicial cases imply that it will be given greater weight during the review if it is corroborated by ocular or physical evidence. Even though it is now general knowledge that such evidence can be produced in court, this remains the case. If Pakistan is serious about protecting digital evidence, it must adopt regulations about custody, accessibility, authenticity, and validity. The judge had broad discretion in determining whether or not to hear such evidence. These components are now considered secondary evidence; therefore, they must be supported by primary evidence. When an audio recording is used in court as evidence, for example, both the recording equipment and its operator must be present. The legislative branch has lately ruled digitally-created documents admissible as primary evidence. QSO's expansive view of "evidence of the document" permits a variety of media, including handwritten notes, digital data on a hard drive or USB flash drive, and emails. Digital evidence was historically considered secondary evidence since it required additional resources, such as a printer, to produce a form that could be viewed by people.

Due to recent revisions in the law, however, it is no longer considered hearsay. The advent of ETO 2002 has rendered the acceptance of such evidence uncontested; nonetheless, different judicial decisions indicate that it will be accorded greater weight during evaluation if it is corroborated by optical or physical evidence. The publication of ETO 2002 has made it apparent that such evidence can and should be used, but if it can be supported by other sorts of evidence, such as direct observation or physical objects, it will be accorded a great deal more weight. It is essential to question the validity of this line of thought. As the prosecution's use of this form of evidence increases, so should our judges' familiarity with it and the notion that it should be treated the same as oral or written primary evidence if any alterations, deletions, or storage conditions can be persuasively justified at trial. Even if digital evidence is acceptable in Pakistani court proceedings, the country must still enact regulations and laws to protect its integrity and reliability. When your claims are supported by evidence, you can reliably predict how they will fare in court. There is also a great deal of discussion and disagreement regarding the correct classification and labeling of digital evidence. By following the court's lead on the admissibility of digital evidence, the trial proved that there is still considerable skepticism regarding the reliability of digital evidence in court. The 1984 modification of the QSO by the Pakistani parliament to permit the use of digital evidence made this an actual reality. The Electronic Transaction Ordinance is another piece of legislation from 2002 that illustrates Pakistan's prominence in this field. It is highly uncommon for a court to rely only on digital evidence, and the majority of judges still require extra proof to authenticate digital evidence.

Clarification on Data Availability

All contributors to the listed articles are strongly encouraged to make their raw data accessible to the academic community. Google Scholar publications give us access to the datasets we utilized or created for our research and any other relevant information that could be used to verify the study's conclusions. If no conflict of interest is possible, write "the authors declare no conflict of interest." Authors are accountable for fulfilling their commitments. It must be made explicit whether the sponsors participated in the study's conception, method selection, interpretation of results, drafting of the paper, or decision to publish the results.

References

Ahmed, D. G. (2021). *Digital Evidence and the Administration of Criminal Justice*. Blackstone School of Law & Business. https://www.bsolpk.org/digital-evidence-and-the-administration-of-criminal-justice

Bartels, B. L. (2022). Courts and public opinion: a critical review. In *www.elgaronline.com*. Edward Elgar Publishing. https://www.elgaronline.com/view/book/9781800379619/book-part-9781800379619-42.xml

Cross, S. P., Karin, E., Staples, L. G., Bisby, M. A., Ryan, K., Duke, G., Nielssen, O., Kayrouz, R., Fisher, A., Dear, B. F., & Titov, N. (2022). Factors associated with treatment uptake, completion, and subsequent symptom improvement in a national digital mental health service. *Internet Interventions*, *27*, 100506. https://doi.org/10.1016/j.invent.2022.100506

Das, S., & Nayak, T. (2013). IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(2), 142–153. https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf

Dudhe, P., & Gupta, S. R. (2022). Machine Learning Approaches in Mobile Data Forensic: An Overview. *Proceedings of the Third International Conference on Information Management and Machine Intelligence*, 93–102.

https://doi.org/10.1007/978-981-19-2065-3_12

Fletcher, E., Hoofnagle, C., Stover, E., & Urban, J. (2013). *AN OVERVIEW OF THE USE OF DIGITAL EVIDENCE IN INTERNATIONAL CRIMINAL COURTS SALZBURG WORKSHOP ON CYBERINVESTIGATIONS*. https://humanrights.berkeley.edu/sites/default/files/publications/an-overview-of-the-use-of-digital-evidence-in-international-criminal-courts-salzburg-working-paper.pdf

Hameed, U. (2021). Admissibility of Digital Evidence: A perspective of Pakistani Justice System. *Pakistan Social Sciences Review*, *5*(IV), 518–530. https://doi.org/10.35484/pssr.2021(5-iv)40

Lewulis, P. (2021). Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law. *Criminal Law Forum*. https://doi.org/10.1007/s10609-021-09430-4

Majeed, N., & Hilal, A. (2022). MEANINGS, CATEGORIES, FUNCTIONS AND STRUCTURE OF PRESUMPTIONS: A STRUCTURAL ANALYSIS OF PRESUMPTIONS IN QANOON E SHAHADAT ORDER. *Pakistan Journal of Social Research*, *04*(01), 451–460. https://doi.org/10.52567/pjsr.v4i1.669

Majeed, N., & Khayal, M. (2022). Exploring Generalizations: A Doctrinal Analysis of Meanings, Kinds, and its Function in the Judicial Process of Proof. *Pakistan Languages and Humanities Review*, *6*(2), 549–558. https://doi.org/10.47205/plhr.2022(6-II)48

Majeed, N., Hilal, A., Muhammad, R., & Rashed, U. (2022). PROVING FACTS IN JUDICIAL PROCEEDINGS: MEANINGS AND MECHANISM OF PROOF IN QANOON E SHAHADAT. *Pakistan Journal of Social Research*, *4*(4), 734–742. https://pjsr.com.pk/wp-content/uploads/2022/12/78.-Vol.-4-No.-4-December-2022-Majeed-Hilal-Rashed-Proving-Facts-in-Judicial-Proceedings.pdf

Paquet-Clouston, M., & García, S. (2022). On the motivations and challenges of affiliates involved in cybercrime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09474-x

Rasool, N., & Rasool, M. (2022). Challenges for Expert Evidence in the Justice System of Pakistan. *Journal of Forensic Science and Medicine*, *8*(2), 62. https://doi.org/10.4103/jfsm.jfsm_16_21

Saeed, M. A., & Gillani, A. H. (2021). Evidential representation of using the modern devices and decisionmaking feasibility in Pakistan. *Journal of Law & Social Studies*, *3*(2), 79–86. https://doi.org/10.52279/jlss.03.02.7986

Solanke, A. A., & Biasiotti, M. A. (2022). Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. *KI - Künstliche Intelligenz*. https://doi.org/10.1007/s13218-022-00763-9

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things*, *19*, 100544. https://doi.org/10.1016/j.iot.2022.100544

Yallamandhala, P., & Godwin, J. (2022). A Review on Video Tampering Analysis and Digital Forensic. *Proceedings of International Conference on Deep Learning, Computing and Intelligence*, *2*, 287–294. https://doi.org/10.1007/978-981-16-5652-1_24

Zaman, M. S., & Bhatti, S. H. (2023). An Overview of Criminal Justice System to Uphold the Supremacy of Law in a Sovereign State: An International Perspective. *Review of Education, Administration & Law*, *6*(1), 1–11. https://doi.org/10.47067/real.v6i1.300