JOURNAL FOR SOCIAL SCIENCE STUDIES

An International Peer-Reviewed Open Access Journal

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063

Volume 4, Issue 2, June 2026

FROM STATUTE TO COURTROOM: ADMISSIBILITY, JUDICIAL REASONING, AND INSTITUTIONAL GAPS IN PAKISTAN'S TREATMENT OF ELECTRONIC EVIDENCE

Muhammad Ateeq Ashraf[*1], Sonia Aslam[2], Dr. Muhammad Raees Ashraf[3]

[*1,2]*Assistant Professor, School of Law University of Gujrat*
[3]*Additional Director University of Gujrat*

[*1]ateeq.ashraf@uog.edu.pk, [2]sonia.aslam@uog.edu.pk, [3]raees.ashraf@uog.edu.pk

DOI: https://doi.org/10.5281/zenodo.21989579

Keywords
electronic evidence; Qanun-e-Shahadat Order 1984; Prevention of Electronic Crimes Act 2016; admissibility; chain of custody

Article History

Received: 28 April 2026
Accepted: 15 June 2026
Published: 30 June 2026

Corresponding Author: *
Muhammad Ateeq Ashraf

Abstract

Pakistan's criminal justice system has increasingly come to rely on the dependability of electronic evidence (call data records, WhatsApp messages, CCTV footage, forensic disk images) but the statutory "structures" created to evaluate this evidence pre-date the technologies regularly brought to trials. A doctrinal journey from statute to court is traced here. It first charts the overlapping rules of the Qanun-e-Shahadat Order 1984, the Electronic Transactions Ordinance, 2002 and the Prevention of Electronic Crimes Act, 2016. It then looks at how, in if left at large, these open-ended clauses have been worked out in practice by the superior courts, using a Supreme Court decision as an anchor – Ishtiaq Ahmed Mirza vs the Federation of Pakistan – to reveal that meaningful safeguards, such as, the source requirement, the custody requirement, and the need for non-tampering have emerged largely from case law rather than legislation. The article then moves to the institutional level – forensic capacity, the chain-of-custody practice, and judicial training deficits affecting the practice of doctrine-level protections. The article points out that Pakistan would be better served with a statutory authentication checklist that brings together the various case-by-case judicial rules on authentication and makes it available in the public domain, instead of relying on the assumed "trustworthiness" of computer-based technology, like the Indian certification-based process which has proven flawed in that context.

I. INTRODUCTION

Current judicial proceedings are equipped with digital materials, and increasing cases of crime incorporate digital materials. Call data, WhatsApp threads, witnesses and any footage captured by CCTV is an invitation to a suspect to be at the scene of a crime; and forensic images from a seized mobile often do all three. The country's key electronic forensic organization, the Federal Investigation Agency (FIA) Cybercrime Wing, has carved out a niche for itself in addressing these types of issues in regular investigations – it exists because it can no longer be ignored in specialised prosecutions of cybercrime. In a nutshell, electronic evidence has become a mainstay of the criminal practice instead of its outskirts.

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4, Issue 2, June 2026

Not all this law has 'migrated' at the same speed. The Pakistan's main evidentiary codices, Qanun-e-Shahadat Order 1984 ('QSO 1984'), originally was prepared for a world characterised by paper documents, oral evidence and physical exhibits. Since that time it has been patched, not rewritten: initially by the Electronic Transactions Ordinance 2002, which did add a few elements recognising the concept of electronic documents, and finally by the Prevention of Electronic Crimes Act 2016 ('PECA 2016') which placed a new layer of criminalisation and investigation on the document - based offence of the system, primarily for cyber-crime. The end effect is a set of laws compiled at three different points of enactment over a 30-year span – but no consolidating statute that says anywhere, on the record, how to-authenticate and how to weigh electronic evidence to a court for a trial.

This article seeks to address the question of whether in practice that "layered" structure has resulted, in some cases, in a uniform and predictable standard for admitting electronic evidence in criminal trials, or whether they are mainly acceptable to the court because they are novel investigative methods that are unique to police station A versus station B, and forensic lab A versus lab B. The central argument of the party is that the courts of Pakistan have done a lot more than legislatures could possibly have done: a line of cases culminating in Supreme Court's verdict on the authentication in Ishtiaq Ahmed Mirza vs Federation of Pakistan has created a functional test for authentication based on a single open-textured gateway of a statute. But it is not yet realized, because it is something that exists in precedent — not as a checklist — and because the institutions belonging to creating and maintaining electronic evidence, such as investigation agencies, forensics laboratories, and even the trial court, don't yet have enough uniformity to rely on the test.

This article continues with five additional parts. Part II charts the statutory basis of the QSO 1984 up to Article 164, then illustrates the layer of procedure that was transformed following the amendment to PECA in 2002 and subsequent 2016 revision of the PECA itself and other related routine procedures. Part III looks into how the superior courts have invoked the said architecture, analyzing the development of an authentication test by turning to the cases of Ishtiaq Ahmed Mirza and associated cases. Part IV explores institutional deficiency issues of whether or not the judicial test can be achieved on the ground, including issues of forensics, chain-of-custody practice and institutional training. Pakistan's strategy is compared with the compulsory-certificate system adopted in India, and preeceously bug-ridden computer system in England and Wales, lessons learned from each for reform of Pakistan's approach are provided in Part V. The concrete recommendations are provided in Part VI and the conclusions are given in Part VII.

This is no overnight enterprise in which the stakes are philosophical and moral. When the standard is not clear, in the same system two contradictory failures are possible: the courts accept unreliable material since no fixed standard requires some searching inquiry regarding the source nor do they mandate that the searching scope exceed what the higher courts might require; the courts refuse to admit genuine and probative material because the uncertainty of what a trial judge must, in fact, apply as the standard is such that he will resort to a "harsher" standard than any one of Article 164 or its supporting provisions would call for. Both are costly to humanity, in one way and another, a wrongful conviction in the one and the abandonment of a sound prosecution in another; and both are more likely to occur where the underlying rule is only summarized somewhat idiosyncratically in the reasoned judgments that are recorded post hoc on appeal, and not cast in the absolute language of a freely-written statute that everyone in the criminal courts system can read directly.

In terms of methodology, the article is of the doctrinal type. It relies on the fundamental texts

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4, Issue 2, June 2026

of the QSO 1984, Electronic Transactions Ordinance 2002 and PECA 2016, along with reported case law decided by the Supreme Court and High Court in these countries against specific examples of these texts, with the narrower and purpose chosen from India and England and Wales being chosen because they offer structurally different solutions to the same authentication problem which Pakistan's courts have discussed in case law, namely, mandatory certification, and rebuttable presumption. The analysis is not an empirical description of the experience of court practice in the tribes, particularly as revealed by trial data; if trial data is used, it is handled with care, and any shortcomings of the source of data are indicated.

II. The Statutory Architecture

A. A Pre-Digital Code Meets a Digital World

QSO 1984 has substituted the colonial periods Evidence Act 1872 and has shifted away from the concept of strict and binding relevance rules and shifted the law of evidence in Pakistan to general rules of relevance, primary and secondary stream of evidence, and expert opinion in accordance with Islamic evidentiary principles. The drafters did not at the time consider call data records or logs of discursions during IM or think to mention their treatment in the Order. Two later interventions toppled that: one incidental provision in the original 1984 text and a "package" of 2002 amendments which provided a statutory support structure for it.

B. Article 164: A Gateway, Not an Authentication Code

Article 164 of the QSO 1984 provides that it may authorize the use of evidence which has come into existence with modern devices or techniques in court cases it deems suitable. Over time, the courts have interpreted this as rather expansive, meaning that any technology in existence may be included – audio cassettes for the 1990s, CCTV footage and mobile phone data for the present day. The Peshawar High Court in one of the earliest reported cases ruled admissible a recording on an audio-cassette under this gateway. One of the advantages of the article becomes is also a liability, it leaves room for courts to choose their own procedures, and it is open-ended to allow for flexibility. It does not differentiate between evidence and modern devices and does not inform a trial court how it must satisfy itself therewith that the recording is proper, unaltered and correctly documented. Case law was left to fill in the details, as Part III indicates.

C. The 2002 Amendments: Relevance, Status, and Proof

The Electronic Transactions Ordinance 2002 was first electronic transaction-specific law of Pakistan, aimed at providing a set of laws for the implementation of electronic commerce. It provided the QSO 1984 with at least the mechanism it was missing in Absentia Act 164, in three interconnected amendments. Relevance is defined in Article 46-A, which states that information, whether produced, received or recorded by an automated system, shall be relevant if the information is generated, received, recorded by an automated system that does not require active human intervention. An added explanation to Article 73 discusses the evidentiary value and states that electronic and digital records will be considered as first hand documents not second hand documents. Article 78-A deals with proof: establishes how the electronic signature and electronic document will be proved. Together, these three provisions address three different questions – is it relevant, what kind of evidence is it and how is it established? – which Article 164 did not answer. Later cases like Mian Khalid Pervaiz v The State would take the support of this composite provocation and not Article 164 alone.

D. PECA 2016: From Facilitation to Criminalisation

Electronic transactions were permitted by the Ordinance of 2002 but PECA 2016 makes their misuse illegal. It established on 11th August 2016

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4, Issue 2, June 2026

and began eight days later, types of crime which ranged from 'Unauthorized Access to Information System' via to 'Cyber-terrorism' and an investigative and prosecutive process. Rights to designate an investigation agency (in practice the FIA) for offences of the Act under section 29 and express direction of its task from section 29(3) give the Federal Government authority to assist with the establishment of forensic analysis capacity, which expressly excludes a forensic report being considered an inadmissible document just because it was produced by section 29(3) of the Act, in itself, by the designated investigating agency. This goes against the usual practice set out elsewhere in the QSO 1984 and the Code of Criminal Procedure that the evidence be made by a person outside of the investigative team. A discussion of this tension follows in Part IV, as it returns to the independence test which courts have subsequently evolved.

PECA 2016, however, is not an evidence law standalone. Under section 2(2) where it adopts a term which is not defined on its own, the meaning of the term has been defined in Pakistan Penal Code 1860, Code of Criminal Procedure 1898 and/or QSO 1984. In other words, the Act is considered best not to be a replacement for the base of evidence laid down by the QSO 1984, but an extension of and a criminalisation of it. Admissibility issues at trial thus go back through Article 164 and the amendments made to the article in 2002, even if the offence is being prosecuted under PECA 2016.

E. The Surrounding Procedural Layer

There are three more provisions to complete the picture of this part of the Compensation Program. Disclosure, as it does with paper records, applies to digital records under Section 265-C of the Code of Criminal Procedure 1898.Whereas the usual rules of disclosure apply to a paper record, disclosure also applies to a digital record in accordance with Section 265-C of the Code of Criminal Procedure 1898. As an alternative to the incorporation of Article 164, a parallel admissibility procedure for electronic evidence in terrorism cases is provided for in Section 27-B of the Anti-Terrorism Act 1997. At least for one province, section 9(3) of the Punjab Forensic Science Agency Act 2007 recognizes an expert appointed by the Agency under this Act as an expert for the purpose of section 510 of the Code of Criminal Procedure and Article 59 of QSO 1984.

F. Judicial Notice as a Parallel Route

Article 164 has also been invoked in a way other than to verify a particular exhibit, that is, for purposes of forming a general impression of the surrounding facts of a case in the light of "things that were reported at the same general time by both the electronic and print media. While this is a narrower use than the admissibility question which takes up the remainder of this piece – this one has to do with background context and not proof of a fact in issue – such is the span the single residual clause in Article 164 has been stretched across, covering a judicial-notice function as well as an evidentiary certificate function, but not with any textual elaboration of the line between the two.

Of course, Part II's survey shows that there's never been a single definitive code of authentication, as Part II's instruments are not bound together into a unified code. That fragmentation is one that is more easily managed when each provision goes in the same direction; however, it involves a great deal of interpretation for both the trial and appellate court, which will be explored in Part III.

III. Judicial Reasoning: Translating an Open-Textured Provision Into a Working Test

A. Ishtiaq Ahmed Mirza and the Emergence of an Authentication Test

The task of authenticating modern-device evidence was left unaddressed in Article 164 and, thus, to the judiciary, where the fount of all knowledge is the decision of Supreme Court in Ishtiaq Ahmed Mirza v Federation of Pakistan. Three errors recurred in the preparation and preservation of the tape and transcript by persons closely involved with as opposed to separate from the party using them, as well as a failure to demonstrate by proper identification that the voice or picture on the tape is that of the person alleged.

The reason for this is that the reason is not so much the actual facts it contains, as the structure it provides. The courts have transformed the broad discretion in Art. 164 into three tests for the application – sources of the work free from connection with other sources, integrity of custody and preparation, and reliable identification, without tampering. Even if there is no legal requirement for a certificate, the function of that test in substance is that of Pakistan's judicially created equivalent of a requirement of certification under the law.

B. CCTV Footage and the Production Requirement

In a similar circumstance, the SC in the case of Asfandyar v Kamran and another has ruled that genuineness of CCTV footage can be proved only by the examination of the person who prepared or operated the CCTVs as a witness. The result is that the recording of CCTV is treated as evidence for living authentication, but not as a self-proving document, giving effect to the independence and custody strands of the Mirza test in a different context which perhaps strengthens the position.

C. Digital Documents as Primary Evidence

It is observed that in Mian Khalid Pervaiz v The State, the Supreme Court instructed that the relevant procedures of QSO 1984 (including Article 46-A with a direct reference to the relevant provisions of the Electronic Transactions Ordinance 2002), were to be followed and the doctrine of composite statutory structure was applied directly to decide that digital documentary evidence was admissible under Article 164 of the QSO 1984, together with Article 46-A and Article 78-A of the QSO 1984. A like usage of the modern-devices gateway can be found in the documentary-devices and device-derived material in Muhammad Irfan vs The State as now the courts do not refer to Article 164 or to the specific support provisions introduced in 2002 separately; instead the three parts are viewed as part of a whole.

D. Tightening Chain-of-Custody Scrutiny

The judiciary has been tightening the 'custode strand' of the Mirza test in the more recent decisions of the High Court, of Sindh. Using the precedent of two cases, Ishtiaq Ahmed Mirza and on Muhammad Rahim Swati v The State, the Court has set the standard for the origin of an audio or video recording to be a demonstrative proof of its origin (that it is not tamper-proof), and for the production of the recording to be made by the person who produced it. In one of those cases, a mobile device bearing an incriminating audiotape passed through a series of custodians without having any of their rightful interests served in any way.In one of those cases, a mobile device containing an incriminating voice mail message had been through a number of hands none of which had been legally shown to have been accorded with any type of rightful interest. The Court in that regard relied on the precedent that was set by earlier cases before it in the Supreme Court such as Riaz Ahmed v The State, Muhammad Asif v The State and Khalid alias Khalidi and two others v The State.

E. An Unwritten Code, Applied Unevenly

Read independently (Parts III.).A to III.D demonstrate that under incremental evolve case law, a working "statutory certification system" has been developed by Pakistani courts, consisting of three key components: independence of source, integrity of custody and reliable identification with an added, increasingly stringent chain-of-custody requirement. Article 164 is subsequently discretionary and its test exists, therefore, in precedents, not a checklist, which means that how it is applied at trial level varies accordingly. Discussing these digitally-made standards as contained in Pakistani case law, commentators have advocated for codification, and, at least one review of digital-evidence practice in Pakistani courts reveals that a "consistent" standard has been far from the practice of courts at the trial level in recent cases, with a significant percentage of digital evidence tendered rejected on procedural grounds. In Part IV, the conditions of the institutions are explore as contributing factors to that unevenness.

F. Admissibility Is Not the End of the Inquiry

It is worth stopping on a distinction that sometimes lapses the case law. The satisfaction of the Mirza test determines whether a recording, transcript or electronic report on a document is admissible to the court and cannot alone determine the weight to be afforded it when admitted into evidence. Just as a properly proved paper document can be given limited probative value, a recording that has overcome the independence, custody and identification requirements may, nevertheless, be given limited probative value just because it is inconsistent with the other evidence is not enough to establish that it is not.A properly proved paper document can be given limited probative value, and a recording that does so may, too, be given limited probative value only because it is inconsistent with other evidence, or only because it is incomplete or only because it is susceptible of an innocent explanation. Applying "admissible" to "weighted" is bound to produce two dangers: that the Mirza test will be used as a filter to exclude the most important kinds of evidence that a jury or trial judge ought to consider to be reliable, or that the evidence which is admitted will simply be taken as incontrovertibly true because it is admitted. The two questions have been broadly kept apart in Pakistani appellate practice but this is an issue that needs to be emphasized, in any new codification endeavor, as an admissibility checklist that is drafted with just that question in mind is dangerous of being construed, by the trial judge, as also deciding the question of weight.

IV. Institutional Gaps: Where Doctrine Meets Capacity

A. Forensic Infrastructure

The judicially formulated criteria outlined in Part III is based on an investigative and forensic ship equipped to operate in a fashion that conforms to such requirements, namely independent custody and handling of items and technically competent examination. The main specialized unit in this regard in Pakistan is Cybercrime Wing, Federal Investigation Agency, who states that it is the only cyber special wing in the country, experts in digital forensics and technical investigation, in information-system security audits, and penetration testing. Statically, the Punjab Forensic Science Agency is providing similar capacity at the provincial level and has been recognized as experts under the code of criminal procedure and under the QSO 1984. Specialist forensic capacity, as focused in one federal unit and one provincial agency, however, means that, when using the Mirza test, the lack of a provincial equivalent does not significantly affect a province's ability to carry out the delivery of evidence; with a less stringent evidentiary test, those factors might have a greater impact.

B. The Self-Certifying Investigator Problem

A structural tension is there which needs to be made explicit both in part II and Part III. PECA 2016, Section 29(3) does not require the forensic report by the investigation agency to be rendered on the basis of inside expert systems but the agency's own forensic report as accepted without needing to file it as an “improper” document. The Mirza test, on the other hand, makes any evidence, like a recording or transcript, considered by forensic reports to be independent of the interested party a threshold requirement for the evidence's authenticity. This may create an imbalance: the evidence collected by the prosecution's own investigative body may meet a lesser level of institutional independence standard than the evidence produced by the private party – an imbalance which may have clear ramifications on the equality of arms guaranteed by Article 10-A of the Constitution of the Islamic Republic of Pakistan 1973. This is not a reason for repealing the section 29(3) whose purpose is to provide for the development of in-house capability for the dedicated agency and is required, not indefinitely but at least as stringently as is Mirza's disclosure obligation for private recordings.

C. Defence-Side Capacity and Judicial Training

There is another imbalance between the prosecution and the defence. Although defence counsel have a duty formally to challenge the prosecution's case, it is hard in practice for defence counsel in most districts to have the same easy access as the FIA and provincial forensic agencies to independent custody examination and digital forensic examination capability and expertise in order to then challenge that view. Indeed, this disparity is exacerbated by the lack of uniformity in training provision in relation to the technical aspects of digital evidence for trial judges, which may account for some of the inconsistencies found in the application of Part III.E and mentioned in the comments of those dealing with the challenges of implementing PECA 2016

D. The Best Evidence Rule in a Digital Context

Another snag in the institutional arrangement arises from the readability of the digital documents as primary evidence in Article 73's explanation. A paper original is a single piece of paper; a hard drive is a single disk image and can be replicated in any evidential manner without loss of fidelity. This is suitably recognised by Article 73's categorisation of electronic documents as primary evidence; the same protections therefore are no longer provided by the difficulty in manufacturing and in making undetected alterations of a definitive document. The responsibility for integrity is virtually completely transferred to custody practice: hash values, keeping write blocked during imaging, and documented chain of custody from seizing the files to the courtroom. The municipality where it does not exist as on the whole, Part IV.A and IV.Whereas C had argued that the formal status of digital evidence as "primary evidence" in the formal categories of the FIA is becoming more common than it is being effectively utilised in the field, the formal designation of digital material as primary evidence may simply chase the institutional capacity that can make this designation useful.

V. Comparative Perspective: Lessons From Certification and Presumption Models

A. India's Mandatory Certificate

In Anvar PV v PK Basheer, the Supreme Court of India has emphasized that together with section 65A itself, section 65B contains a comprehensive framework for the admissibility of electronic records to be admitted as secondary evidence and that a signed certificate under section 65B(4) is a condition precedent to admission of an electronic record tendered as secondary evidence. The mandatory nature of the certificate was reiterated by a three-judge bench in Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal, but the court clarified that it was not necessary to have the certificate read at the very beginning of the proceedings; that the court could order the reading of the certificate when a party refused to produce it; that there was no need for a certificate to be read where the original certificate device – not a copy – was presented and proved by the registrar or operator. In India, therefore, judicial flexibility is being surrendered for the certainty provided by statutes: either the certificate is complied with or it isn't.

It costs to be predictable. Whereas, commentators lax in Indian practice under section 65B have felt that this has resulted in the exclusion of electronic evidence in too many cases, and believe that prosecutions would fail based on mere technical non-compliance with this requirement, even if the underlying documents have not been seriously challenged as evidence of their genuineness. Therefore, a mandatory certificate regime is an adequate remedy to the uncertainty which Part III

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063

Volume 4, Issue 2, June 2026

points out in Pakistan's case-law approach but would be done at the cost of form over substance.

B. England and Wales: The Danger of an Unrebutted Presumption

The other extreme is seen in the history of England and Wales. The Law Commission proposed that section 69 of Police and Criminal Evidence Act 1984, which imposed a requirement for evidence of the proper working of a computer before it could be used to produce evidence, should be abolised and should instead be presumed to have worked correctly at the time of production (unless there is evidence to the contrary). This would be more of a burden for the party seeking to prove malfunction—something that would later be hard to do in practice, especially in prosecutions that were based on breaches in accounting software that would not result in the presumption of reliability being overcome for years after the wrongful conviction. The English experience warns against doing everything it can to overreach Pakistan's problem of unpredictability by trying to go too far the other way and assume reliability.

A third comparator (outside the immediate context of South Asian and common law English) underlies the argument. While the intent of Article 164 and/or section 65B is echoed in commentary, it does not identify the absence of an admissibility rule as the main hurdle to having reliable outcomes, but rather that there is no settled protocol for how electronic evidence is captured, stored and presented. The observation can be extended above South Africa; whatever an admissibility model adopted in a country is, it cannot do without procedure and institutional foundation, which is the lacunas Part IV highlights in Pakistani context.

C. A Middle Path for Pakistan

Currently, Pakistan is in the middle of these two points. Unlike the historical English position (which was a trust presumption that the results of the certificate did not have to be repeated before conviction was obtained), Article 164 does not include such a presumption in favour of the prosecution, but it does give courts discretion that a certificate is not required to obtain a conviction. Judicial elaboration via Mirza, Asfandyar and the jurisprudence of the Sindh High Court on the custody has brought in a sort of 'standard of authentication' which is essentially same in substance as the Indian certificate requirement, but lacking the Indian legislativeness in determining when the standard has been met. Comparative lesson is not this wholesale Pakistan should endorse, but this Pakistan's own institutions have arrived at a balance, which can be built flexibly to ensure that it does not become rigid like India while at the same time it does not become over-corrective, like England earlier.

VI. Towards a Coherent Framework: Recommendations

The analysis given above entails four reforms. First, the three-part test in Ishtiaq Ahmed Mirza which brought the field of custody jurisprudence to its present level of refinement and definition in the subsequent decision of the Sindh High Court must be laid down as an explicit authentication checklist in the relevant QSO 1984/PECA 2016, as the trial courts and investigators will now have to point to an easily accessible standard and not have to dance to the tune of the constantly evolving body of the precedent, without having access to all of it.

Second, the tension as emerged and defined in Part IV.Another approach – direct, rather than by a repeal of the forensic capability of the investigating agency – would be to introduce a statutory disclosure requirement with the same independence obligations that are already in place as regards private recordings – where the forensic agency should place all its methodology, chain-of-custody documents, and any findings, upon whose basis they cannot be challenged, within the hands of the defence.

Third, the provincial forensic capability needs to be developed beyond the narrow scope of the

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4, Issue 2, June 2026

currently focussed federal FIA and the Punjab Forensic Science Agency, and the standard operating procedures need to be captured in a provincial manner to ensure that the reliability of an authentication finding shall not be dependent on the province where the offence was investigated.

Fourth, there is a need to extend standardisation on the technical and evidentiary aspects of digital evidence, as opposed to the lack of uniformity at the trial level shown in part III.The resource disparity on E and for the prosecution and defence sources of forensic expertise raised in Part IV.C.

Fifth, any codification exercise should leave the distinction detailed in Part III intact.Between the question of admissibility and weight, so that a future statutory checklist governs only the question of what a court may admit, and the question of how much a trial court should rely on admitted material to the ordinary principles of apprising evidence. The former, a collusion that leaves an unsuspecting court to its own devices to evaluate unadmitted facts of material importance, and the latter, an unwarranted presumption of reliability, the sort that abetted in the English experience mentioned above in Part V.B.

VII. Conclusion

That journey starts with a single, intentionally non-specific provision in an evidentiary code promulgated in 1984; then a package of 2002 amendments that 'legislatively' gave that clause teeth and finally into a court room where judges have been tasked with, case-by-case, creating the evidentiary standard that the legislature never attempted at all to codify. That judicial triumph based on the cases of Ishtiaq Ahmed Mirza (in the absence of anyone otherwise) before Federation of Pakistan and further developed in the recent custody cases of the Sindh High Court, is very real and palpable. It is also incomplete, in so far as it relies upon institutions which have widely differing capacities nationwide -- forensic laboratories, investigating agencies and trial courts -- and in so far as it continues to be dispersed throughout precedent and not in a single readily available statutory document.

None of that detracts from what the judiciary already has accomplished. Today's court reading is not the same as one that has access only to Article 164. In reading the trajectory of development that has existed in Parts II through IV – from bare residual clause to a supporting package of relevance, status, and proof provisions to a "judicially-crafted authentication test" to an evolving chain-of-custody jurisprudence – one of the most discernible features is the continued maturation of the doctrine, albeit at times fitfully. Some of the work on the reverse side of the coin is more a case of consolidation and capacity-building – the writing of what the courts have determined, the closing of a gap with respect to the independence of the courts in section 29(3), and of making sure that the standard set by the court by that section is met by all provinces, not just those where well-resourced forensic agencies already exist.

This article's thesis is modest, therefore, and is to the effect that Pakistan does not need primarily a new law entitling electronic evidence. Its mandate is to document in one place what the law is that it has established in itself, and then ensure that the law is implemented at least as it is in its own courts, in terms of institutional capacity – forensic infrastructure, disclosure that can be made with the assistance of the Defence, and judicial training – from one courtroom to the next. The admissibility clause for electronic evidence in a criminal trial in Pakistan is not only that it has a nexus with the conduct of what took place, but also which court gains jurisdiction to admit it in a criminal trial.

Bibliography

Legislation

Constitution of the Islamic Republic of Pakistan 1973

Qanun-e-Shahadat Order 1984 (P.O. No. X of 1984)

Code of Criminal Procedure 1898

ISSN (Online): 3006-2071 | ISSN (Print): 3006-2063
Volume 4, Issue 2, June 2026

Anti-Terrorism Act 1997
Electronic Transactions Ordinance 2002 (Ordinance LI of 2002)
Punjab Forensic Science Agency Act 2007
Prevention of Electronic Crimes Act 2016 (Act No. XL of 2016)
Indian Evidence Act 1872 (India)
Police and Criminal Evidence Act 1984 (UK)

Cases: Pakistan
PLD 1998 Peshawar 52
Riaz Ahmed v The State 2010 SCMR 846
Khalid alias Khalidi and two others v The State 2012 SCMR 327
Asfandyar and another v Kamran and another 2016 SCMR 2084
Muhammad Asif v The State 2017 SCMR 486
Muhammad Irfan v The State and another 2018 P.Cr.L.J 1319
Ishtiaq Ahmed Mirza and 2 others v Federation of Pakistan and others PLD 2019 Supreme Court 675
Mian Khalid Pervaiz v The State 2021 SCMR 522
Muhammad Rahim Swati v The State 2024 YLR 1636

Cases: India
Anvar PV v PK Basheer (2014) 10 SCC 473
Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1

Secondary Sources
ASAD & BASIM Advocates & Legal Consultants, 'The Qanun-e-Shahadat Order, 1984: Its Role in Civil and Criminal Trials and Practical Significance for Legal Practitioners' (ablawfirm.org, 9 March 2025)
Christie J, 'The Presumption in England and Wales that Computer Evidence is Reliable – Time for Action' (clarotesting.wordpress.com, 22 March 2024)
Federal Investigation Agency, 'Cybercrime Wing' (fia.gov.pk)
Iqbal M, Talpur SR, Manzoor A, Abid MM, Shaikh NA and Abbasi S, 'The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan' (2023) 2(4) Siazga Research Journal 273
Law Commission, Evidence in Criminal Proceedings: Hearsay and Related Topics (Law Com No 245, 1997)
MIT Cyber IR, 'Challenges Faced by the Judiciary in Implementing Cybersecurity Laws in Pakistan' (cyberir.mit.edu)
Rana AA, Naul AH, Gujjar UA and Ahmad FZ, 'Admissibility and Evidentiary Value of Electronic Evidence in Criminal Cases: A Case Study of Pakistan' (2022) 4(1) Journal of Law and Social Policy 27
RostrumLegal, 'Threshold Admissibility of Electronic Evidence: Anvar and Thereafter' (rostrumlegal.com, 16 April 2023)
United Nations Office on Drugs and Crime, Electronic Evidence Country Fiche: Pakistan (UNODC)