INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909

Volume 4, Issue 3, 2026

THE DEEPFAKE DILEMMA: A TIERED JUDICIAL STANDARD FOR AUTHENTICATING AI-GENERATED EVIDENCE UNDER PAKISTANI LAW

Dr. Miftahuddin Khilji[*1], Barak Allah[2]

[*1]*Assistant Professor, Department of Law, International Islamic University, Islamabad*
[2]*LLM Human Rights Law Scholar International Islamic University, Islamabad*

[*1]miftahuddin.khiji@iiu.edu.pk, [2]02153llmhrlf25@student.iiu.edu.pk

Corresponding Author: *
Dr. Miftahuddin Khilji
DOI: https://doi.org/10.5281/zenodo.22975035

Received	Accepted	Published
01 January 2026	17 March 2026	31 March 2026

ABSTRACT

The advent of generative artificial intelligence has now allowed the creation of photographic, video, and audio evidence of a quality that can be easily challenged, posing a critical threat to the courts in Pakistan and other countries. When a court declines disputed audio-visual content without sufficient justification, a real litigant or victim will have been deprived of a lawful remedy; when it permits disputed content to pass without sufficient verification, a court may be making a legal decision or conviction based on a fake. The paper discusses how the current evidentiary architecture in Pakistan, which is mainly the Qanun-e-Shahadat Order 1984, the Electronic Transactions Ordinance 2002 and the Prevention of Electronic Crimes Act 2016, as amended in 2025, remains relevant but is incomplete for wholly synthetic evidence, and the aim is to address this predicament. The paper, based on statutory text, reported case law, and existing Pakistani legal scholarship holds that provenance, chain of custody, integrity, and non-tampering considerations used in Pakistan are incomplete to deal with the wholesale synthetic fabrication, as they were originally created in a pre-generative-AI context. It suggests a more graded judicial authentication criterion - a threshold proponent burden, a burden-shifting burden on true challenge, institutionalized judicial gatekeeping, and an institutional forensic backstop - designed to minimize and reduce erroneous exclusion and erroneous reliance without necessitating wholesale new law.

Keywords:

Deepfake evidence, AI-generated evidence, Electronic evidence Pakistan, Evidentiary authentication, Qanun-e-Shahadat Order 1984.

INTRODUCTION

Artificial intelligence powered tools that can produce or edit photographic, video, and audio media, which are often referred to as deepfakes, transitioned out of the realm of a research interest and became a common aspect of everyday life. What started as a technical demonstration has come to be involved in political disinformation, non-consent intimate pictures, financial fraud, and, more and more, lawsuits

themselves. It has not spared Pakistan. In February 2025, three first information reports were registered in Lahore, after purported AI-generated videos and photos depicting a senior provincial official in a false light were circulated online, where the complaint behind it was corroborated by a social media link and its contents provided as evidence against it. The incident in question is representative of a larger-scale issue as opposed to a lone issue. When the technology to produce a plausible recording becomes widely accessible, all recordings, natural and artificial ones, are challenged in principle. The fact that photographs, audio recordings and video footage consistently have been treated by courts as abnormally persuasive evidence simply because such evidence seems to be a mechanically captured image of reality and not a fallible human witness has the courts forced to consider the possibility that it is the apparent mechanically objective character of such evidence that is an illusion, itself subject to manufacture. This generates what this paper describes as the deepfake dilemma a court that encounters disputing audio-visual evidence must decide between two current threats of injustice. When it does not accept the evidence, either because it cannot be positively established, or because its establishment would be costly or difficult beyond the resources or expertise of the court and the parties themselves, a party having true, probative evidence will be deprived of a just result. When it takes the evidence without subjecting it to careful consideration, there is risk that the court will be made a fool by a fabrication with repercussions that include erroneous civil responsibility and erroneous criminal conviction. Both mistakes are unacceptable and the risks can not be easily traded off against each other by altering one threshold; the trick is that the verification process must be well-built to make a practical distinction between the two scenarios.

2. Statement of the Problem

Pakistan's legal framework governing electronic evidence has evolved incrementally through the Electronic Transactions Ordinance, 2002, the Qanun-e-Shahadat Order, 1984, and the Prevention of Electronic Crimes Act, 2016, as subsequently amended, including through the 2025 amendments. The existing framework provides a legal basis for the recognition, admissibility, and forensic examination of electronic records, including digital documents, audio and video recordings, mobile-phone data, and other electronically generated information. Nevertheless, its evidentiary architecture has largely developed around the conventional problem of establishing the authenticity and integrity of an existing digital record—namely, whether the record can be attributed to its purported source and whether it has been altered, modified, or tampered with after creation. The emergence of generative artificial intelligence and deepfake technologies presents a qualitatively different evidentiary problem: a recording may possess the appearance of an authentic and untampered digital file while nevertheless being entirely synthetic and unrelated to any underlying real-world event. Recent Pakistani scholarship has therefore identified a significant gap between conventional mechanisms of electronic-evidence authentication and the emerging need to establish the provenance and reality of AI-generated or AI-manipulated content.

A recent study notes that the National AI Policy of Pakistan covers digital literacy but does not cover technology manipulation, the existence of clear evidentiary standards to cover digital crime, and that the deepfakes themselves are the result of technology manipulation of reality independent of the intent of the disseminator, and that the 2025 amendment to the Prevention of Electronic Crimes Act does not cover the technology itself, but the intent in which it was disseminated, which is structurally inadequate since deepfakes are the result of technological manipulation of reality, irrespective of the intent behind the dissemination of that very content.

This is not a mere rhetorical gap in the literature: it is always the insufficiency of the current framework that existing Pakistani commentary recognizes, but never goes any further than

indicating that there could be an operable evidentiary test that could actually be applied by a trial judge when challenged audio-visual material is tendered. The paper seeks to fill that gap.

3. Research Questions

1.Adequacy of Pakistan's statutory/judicial framework for authenticating AI-generated or AI-manipulated audio-visual evidence?
2.The competing risks of excluding genuine evidence and relying on fabricated evidence, and their effect on fair trial/access to justice.?
3.Development of a tiered judicial authentication standard within the existing evidentiary framework.?

4. Literature Review

Deepfakes-related legal research in Pakistan is still nascent and recent, and has emerged in parallel with the global wave of interest in this topic after the mainstreaming of generative AI tools since 2022. A comparative piece released by the Lahore University of Management Sciences law journal places Pakistan's shortcomings in relation to the statutory protection afforded to personal likeness in Denmark, contending that Pakistan has a framework to protect against the harms of disclosure of personal likeness as well as the harm of disinformation but not the harm of technological impersonation. A related issue is discussed in a separate article in Sarhad Journal of Legal Studies titled "The crisis of legal authenticity," which addresses the potential impact of synthetic media on already existing principles of evidence, privacy and accountability, as well as the need for a framework of regulation.
Deepfakes present a serious issue for admissions and authenticity of evidence in legal proceedings, and, as observed by Syeda Samana Ameer in his article in the Research Society of International Law, when once digital evidence corroborated oral evidence, the advent of deepfakes now makes it likely that oral evidence will corroborate digital evidence..
One of the 2025 papers published through the TILS Law Review, however, seeks to focus specifically on the domestic cyber-law gap, noting that the cases that have actually been filed since 2025 PECA amendment is enacted involve misleading information and hate content, not synthetic media in general, meaning that the amendment is more of a speech-regulation tool than a deepfakes-specific law; and that the Federal Investigation Agency's Cyber-crime Wing is under-resourced and lagging in technical expertise from a problem scale perspective..
In a shorter practitioner-oriented section, the same missing link is identified under the Prevention of Electronic Crimes Act 2016, the Pakistan Penal Code 1860, and the Defamation Ordinance 2002, and a few measures are suggested, such as the creation of dedicated units to investigate deepfakes within the Federal Investigation Agency and enhancing the digital forensic capabilities of the National Cyber Crime Investigation Agency.
The common theme in the literature is how the system was not intended for generative AI, while the common absence is an answer to the question this paper asks: What should be the test for a trial judge when the parties have tendered and contested audio-visual evidence, and the other party says it is an AI fabric? The doctrinal basis to answer that question is developed in sections 5and 6 below, and an answer is suggested in section 10

5. The Statutory Framework Governing Electronic Evidence in Pakistan

5.1 The Qanun-e-Shahadat Order, 1984

In Pakistan, the Qanun-e-Shahadat Order, 1984 is the key evidence-based legislations for the reception and proof of electronic evidence. Article 46-A considers as relevant, the statements issued, received or recorded by an automated information system in its normal operation as electronic documents. Article 73 also speaks to the admissibility of electronic outputs as primary evidence (based on two conditions as contained in its Explanations 3 and 4). Article 78-A deals with the case where the attribution of an electronic signature or electronic document is denied, and demands proof of the application of a security procedure. The Court may permit

evidence which has become available by modern devices or techniques under Article 164...
Article 164 leaves ample discretion to courts when receiving evidence made available by modern devices or techniques, but it is essential that evidence is reliable. The origins of the electronic evidence, the manner in which it was obtained and stored, and its integrity in relation to alteration or manipulation may be considered when assessing electronic evidence. The party calling for such evidence should thus be able to prove the source of the evidence and how it was obtained and preserved, especially in the event of its authenticity or reliability being disputed.5.2 The Electronic Transactions Ordinance, 2002
The Electronic Transactions Ordinance 2002, in addition to the Qanun-e-Shahadat Order, is considered as the basic law on digital evidence and cybercrime investigation in Pakistan, as it not only removed the limitation on the validity of the electronic evidence but also held that electronic evidence could be obtained without the need to wait for some independent corroboration to the document. The Prevention of Electronic Crimes Act, 2016, No. 21 of 2016 (Act No. 87 of 1887), as amended..

5.3 The Prevention of Electronic Crimes Act, 2016

In 2025, the Prevention of Electronic Crimes Act was amended with the addition of Section 26A which now criminalises the intentional dissemination, public exhibition or transmission of information which is known, or has reason to believe is false or fake information, and the concept of "aspersion" which refers to the dissemination of information which is false and has a tendency to damage the reputation of an individual..

5.4 The Prevention of Electronic Crimes (Amendment) Act, 2025

In 2025, the Prevention of Electronic Crimes Act was amended with the addition of Section 26A which now criminalises the intentional dissemination, public exhibition or transmission of information which is known, or has reason to believe is false or fake information, and the concept of "aspersion" which refers to the dissemination of information which is false and has a tendency to damage the reputation of an individual..
The 2025 amendment is important for this paper for two separate, if conflicting reasons. However, on the other hand, it is the most 'deep fake adjacent' provision that Pakistani statute law has at present, as fabricated AV evidence presented as real could in theory be considered as the dissemination of false information offence. On the other hand, the amendment itself was designed to cover the problem of disinformation and reputational harm, and not just the ones of evidentiary authentication, and it has been the subject of consistent criticism on this basis..
Human rights groups have criticized the vaguely-worded and ambiguous language in the amendment, citing Pakistan's past occasions of using the Prevention of Electronic Crimes Act against journalists and dissenters to try to suppress legitimate online expression..
The amendment also expanded the definition of "person" to cover state institutions and corporations, which critics say could enable powerful state actors to use the provision to criminalise ordinary people and journalists for disseminating "false information"..
In this context, what is important is the structural difference, not necessarily the political one: a provision designed to control the dissemination of falsehoods is not a proof authentication standard, and superimposing the amendment's contested, speech-restrictive nature over what is ostensibly a technical question of proof is problematic..

5.5 The Constitutional Dimension

Court decisions have determined that recordings without the consent of the person recorded would be a violation of the constitutional right to privacy under Article 14, and recordings made without a verified source or identifiable owner would not count as criminal evidence, but that recordings are considered depending on their

authenticity, chain of custody and freedom from tamper.

It is relevant to the deepfake conundrum because it is the doctrine of this constitutional layer that already provides a significant overlap of source, custody, and manipulation safeguards with the ones that an authentication standard for artificial media would provide.

6. Judicial Treatment of Electronic Evidence: Case Law Analysis

There is no meaningful case law on AI-generated deepfakes reported from Pakistan, which is indicative of the fact the courts have not yet had to develop a specific test. Where there is case law, there is a significant body of fairly consistent doctrine on the authentication of traditional electronic evidence on which a standard applicable to any particular form of deepfake evidence will be based. With regard to closed circuit television records, in Asfandyar and Another v Kamran and Another the Supreme Court said that it was up to the party who had relied on the records of the CCTV system to examine the person who had produced such records to prove that these records were genuine..

In Muhammad Irfan v. The State, the courts held that the forensic reports prepared by the Punjab Forensic Science Agency are admissible as the experts of the treating agency belong to the class of persons specially skilled in forensic material for the purpose of the Qanun-e-Shahadat Order.

In The State v. Ahmed Omer Sheikh, it was ruled that the unavailability of electronic evidence, like a video recording, from the source from which it was gathered and the failure to have it forensically authenticated as not having been tampered with or altered would impact the admissibility of that evidence and may make it wholly unhelpful.

Older authority shows the same underlying logic applied to earlier recording technologies.

It was decided by the Peshawar High Court in 1998 that a statement on an audio cassette was admissible..

In a separate ruling in 1998, a Compact Disc with a recorded confession made during a Press Conference was accepted as evidence pursuant to Article 164 of the Qanun-e-Shahadat Order, and used in conjunction with other evidence to support the conviction.

More recently, in a case in which the CCTV footage helped in finding and arresting the accused, the Gilgit-Baltistan Chief Court took the footage into account under Article 164..

In a family law case decided by the Lahore High Court in 2017, the court admitted video recording of evidence of alleged domestic abuse, even though Article 164 of the Qanun-e-Shahadat Order was not directly applicable to family court proceedings, holding that there was no prohibition on the family court from receiving such evidence in the modern era after proper verification.

Collectively, this case law creates a fairly consistent three-part practice: (i) The party seeking the electronic evidence must demonstrate its source, often by showing the same person who operated or used the recording device, or by examining the device to determine its source; (ii) the evidence must be presented as being free of tampering, usually through forensic examination; and (iii) the courts exercise broad discretion in accepting or rejecting electronic evidence based on the degree that those first two elements are met. The challenge is that this three-part practice is designed for a world where the careless deletion, splicing or manipulation of an original and authentic recording was a primary concern — a world where "identify the source" and "check for tampering" are good tests. The threat from generative AI is different, it is not something that has been altered, it is something that does not exist. When there was no recording device, asking "who operated the recording device" is almost a category error, as it was a fake recording device and a fake man operated it. This is where the currently existing framework, which up to this point is solid, stumbles. Why Deepfakes Break the Existing Test

7. Why Deepfakes Break the Existing Test

There are three distinguishing aspects of generative AI evidence from the scenario that

existing case law was designed to cover – the tampered-recording case.There are three aspects of generative AI evidence that are different from the scenario it was built to handle – the tampered-recording case.

7.1 Absence of an Underlying Original

Tampering analysis assumes, in principle, that an original copy exists with which to compare the tendered copy, although this might be a complex forensic analysis. There's no original to compare to when it comes to a wholly synthetic deepfake; the only question is whether or not it correlates with anything that actually happened. This changes the question, from comparative forensic analysis – does this copy match the source? – to generative forensic analysis – does this file contain statistical signatures of AI generation? – which is a very different and much more challenging technical question.

7.2 The Corroboration Reversal

As one commentator notes, traditionally, oral evidence has been used to support digital evidence, but with the advent of convincing deepfakes, this dynamic may shift and digital evidence increasingly be used to corroborate oral evidence. The reversal has implications for a court's fact-finding process, as well. The testimony of the senses has always been especially credible, exactly because it is not dependent on the witness' credibility or memory.

When courts can no longer assume that the media is reliable when challenged, litigants have one of the most efficient methods to prove disputed facts removed, and the trial may become longer, more expert-driven, and more expensive a cost that will be borne by those who cannot afford the significant forensic litigation.

7.3 Detection Capability Is Still Developing

At the technical research level, too, deepfake detection is an active field of research – the University of Engineering and Technology, Taxila, researchers pointed out that existing deepfake detection methods are too compute-intensive to be practically employed – and a field of contention.

While researchers in specialist computer science fields are still trying to develop efficient and reliable detection tools, it seems that it is not possible to assume that the trial courts in Pakistan and the FITA units which would need to assist them, have ready access to reliable forensic detection capability today. Any proposed evidentiary standard must be truthful about this limitation, not simply make-believe..

7.4 The Gendered Stakes of Getting It Wrong

The implications of the lack of the standard are not uniform. Multi-jurisdictional research shows that the vast majority of the deepfake videos that are spreading on the internet are pornographic.Multi-jurisdictional research shows that the majority of deepfake video clips spreading on the internet are pornographic in nature, disproportionately targeting women, often public figures.

For Pakistan, this is not just a commercial or abstract issue – it is a direct issue of "non-consensual intimate imagery" (denying redress to the victim when the real evidence is wrongfully excluded) and "wrongful admission of fabricated content" (making the fabricated content look like a judicial finding, as if it were the real content).

8. The Dual-Error Dilemma in Practice

It helps to state the two risks clearly - the appropriate response to each is different and a standard which is geared towards one will exacerbate the other.

8.1 Type I Error: Wrongful Exclusion

Any court that takes such a “cautious” attitude toward evidence that is subject to challenge, such as equating any credible claim of manipulation of the evidence by an AI with disqualification of the evidence altogether, gives a veto to any party willing to assert, however improbably, that evidence that it finds inconvenient somehow isn't real. This risk is no longer theoretical in Pakistan's current context: the same sensitivity towards "fake" content that has led to the filing of a first information report against a valid fake video can be exploited in a malicious manner to

attack real clips of corruption, harassment, abuse etc.

8.2 Type II Error: Wrongful Reliance

On the other hand, a courts with a singular test for tamper and no adaptation may end up allowing sophisticated fake videos to be admitted based on flaky evidence, such as a plausible-sounding chain of custody for the video itself, rather than the more important question of whether the video recorded an actual event. This is not a hypothetical threat either, as the use of AI-generated material for political disinformation and reputation attacks has already been noted in Pakistan.

8.3 Why a Single Threshold Cannot Resolve Both Risks

Since the two errors go in opposite directions, they cannot be jointly minimised by simply shifting one admissibility threshold up or down; an increase in the standard to decrease wrongful reliance will automatically decrease the rate of wrongful exclusion, and vice versa. What is required, however, is a procedure that assigns the burden of generating verification evidence to the party that is in the most position to generate it, at the stage of the proceedings where the dispute actually occurs - the rationale behind the tiered standard suggested in Section 11.

9. A Brief Comparative Glance

It is not a paper that offers wholesale transplantation of foreign law but two comparative reference points are useful in showing the scope of regulatory options open. Denmark has considered the issue using the prism of personal likeness and the right to digital identity, and has proposed that the distinctive features of a person should be covered by legal protection against unauthorized imitation by an AI, which Pakistani commentators have proposed as providing a partial model of filling in the identity-protection gap in domestic law, but which is a solution to the underlying wrong issue, and not the underlying evidentiary issue.

The AI Act of the European Union, in comparison, takes the issue at the creation stage instead of the litigation stage, and obligates the creators of AI systems which produce or modify image, audio, or video content to reveal that the content was created or edited artificially. Such a disclosure-at-source requirement, even though not enforced directly on foreign platforms, would alert how the Pakistani courts consider the existence or lack of provenance metadata when presenting evidence. The moral of the story is not that both models should be directly aped by Pakistan, but that jurisdictions that are grappling with this issue are converging on two complementary approaches; regulating the point of creation (labelling, provenance) and regulating the point of use (evidentiary authentication), and that neither of the two has yet been directly tackled by the current reform project, the disinformation offence in the 2025 PECA amendment.

10. Proposed Framework: A Tiered Authentication Standard for Pakistani Courts

The structure given here is specifically designed to work within the current discretionary language of Article 164 of the Qanun-e-Shahadat Order in such a way that it can be adopted by judicial guidelines, a practice direction by the High Court or even by a benchbook, without awaiting new legislation - as well as where legislative codification would reinforce it.

10.1 Tier One: Threshold Proponent Burden

The party tendering contested audio-visual evidence ought to be obliged to prove basic indicia of authenticity before any such evidence is presented before the court at all: the device or platform of origin, the date and custody chain of production to presentation in court and, where possible, unaltered metadata. This reflects the source-and-custody standard already used in other cases like Asfandyar v. Kamran and The State v. Ahmed Omer Sheikh, but expanded to include the possibility that it could be generated by AI instead of just being spliced or edited.

10.2 Tier Two: Shifting Burden upon Genuine Challenge

A simple claim that evidence may be a deepfake, on its own, ought not to be enough to disregard it - it would commit the Type I error of Section 9.1. Rather, a difficult party must be obligated to discover a particular articulable foundation of the accusation (such as a discrepancy in lighting, audio artefacts, or an unplausible provenance). When that threshold has been reached, it should then be the burden of the proponent to provide forensic verification, such as comparing the hash-value with a known original, or running the data through an approved detection tool, instead of having the challenger demonstrate fabrication on his own, which is usually beyond the capabilities of a lay litigant.

10.3 Tier Three: Structured Judicial Gatekeeping

Courts ought to impose a reliability screening role on contested media before granting it substantial weight of evidence, which is broadly similar to the reliability-gatekeeping role of courts in other jurisdictions, that of determining whether or not the method of verification employed has been tested, is agreed upon by relevant experts, and has an error rate that is known and acceptable. This formalizes and does not replace the discretion already available to Pakistani courts under Article 164 and is in line with the current practice of referring to court-appointed or agency-affiliated forensic experts recognized under Article 59 of the Qanun-e-Shahadat Order.

10.4 Tier Four: Institutional Backstop

All the above levels will not work when the Cyber-crime Wing of the Federal Investigation Agency is not adequately staffed and technically capable of performing or overseeing a deepfake-specific forensic analysis. Accordingly, this paper supports the suggestion that already been proposed in the Pakistani commentary that special deepfake investigative capabilities should be instituted in the Federal Investigation Agency and the National Cyber Crime Investigation Agency, and that AI-oriented training and investment in detection tooling should be undertaken, as a legal standard that the courts cannot practically enforce is not a functioning standard at all..

11. Institutional and Policy Gaps

Two of the structural gaps warrant independent consideration since they are not within the tiered framework itself but can make or break it.

11.1 No Statutory Definition of "Deepfake"

The statute law of Pakistan does not yet specify AI-generated or AI-manipulated media as a specific category of evidence. This is not just a gap in labelling: without some category, courts, investigators, and litigants do not have a common language they can use to determine when the tiered standard suggested above is activated at all, as compared to the standard chain-of-custody test used with traditional recordings.

11.2 Tension between the Disinformation Mandate and Evidentiary Due Process

The Digital Rights Protection Authority established by the 2025 PECA amendment has received content-blocking and takedown authority, the exercise of which has drawn criticism regarding a lack of judicial review and statutory clarification due to the disinformation-control mandate of the amendment and its possible abuse as a tool against lawful speech. An essential difference lies between the determination by an administrative authority, as to the purposes of platform-regulation, that a certain piece of content is false, and the determination by a court, as to the purposes of evidence, that a particular piece of tendered evidence is genuine or counterfeit. Mistaking the two - such as by declaring a determination by a Digital Rights Protection Authority to have the force of law in litigation - would introduce the controversial, speech-limiting nature of the amendment to the factual inquiry and must be avoided. It is precisely with this reason that the tiered standard suggested in Section 11 is

specifically a judicial, but not an administrative, process.

12. Conclusion and Recommendations

The current evidentiary framework of electronic material in Pakistan, which is the Article 164 of the Qanun-e-Shahadat Order 1984, along with the Electronic Transactions Ordinance 2002 and the Prevention of Electronic Crimes Act 2016, was designed to deal with tampering and selective editing of authentic recordings. Generative AI presents a completely new issue: the wholesale production of recordings that do not represent an underlying event whatsoever. The source-and-custody, non-tampering approach in the current case law is still required but can no longer be adequate. This gap has been identified by current Pakistani legal scholarship, but has so far not been suggested to be filled by an operative judicial test - the particular contribution that this paper hopes to make under the form of a four tier authentication standard. Three recommendations follow. The first is that at the judicial end of things the Supreme Court or the High Courts ought to think about giving a practice direction or bench book guidance codifying a tiered authentication standard along the lines suggested in Section 11 which can be accomplished under the current discretionary wording of Article 164 without awaiting a legislative overhaul. Second, legislatively, Parliament can consider a specific amendment to the Qanun-e-Shahadat Order or the Prevention of Electronic Crimes Act that establishes AI-generated and AI-manipulated media a separate category of evidentiary purposes, independent of the general disinformation offence that will be established in 2025, so that evidentiary authentication is not confounded with the controversial policy of speech regulation. Third, on the institutional level, the Cyber-crime Wing of the Federal Investigation Agency and the National Cyber Crime Investigation Agency must receive specific funding, training and detection equipment, as even the most well-developed evidentiary standard is just empty air without the forensic opportunities to implement them. Collectively, these three measures would enable Pakistani courts to administer justice to the litigants in the age of AI deepfakes - both ensuring that real litigants are not unfairly denied access to true evidence, and that the truth-finding of the courts is not unfairly dependent on fake evidence.

REFRENCES

Amnesty International. "Pakistan: Authorities Pass Bill with Sweeping Controls on Social Media." Amnesty International, January 29, 2025. https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/.

Ameer, Syeda Samana. "Deepfakes: A Crisis of Human Rights." Research Society of International Law, April 18, 2024. https://rsilpak.org/2024/deepfakes-a-crisis-of-human-rights/.

Advance Legal Research Forum. Journal of Law & Social Studies 3, no. 2 (2021). https://www.advancelrf.org/wp-content/uploads/2021/12/Vol-3.-No.-2-2.pdf.

Bahria University Islamabad Law Journal. "Admissibility and Evidentiary Value of Electronic Evidence." 2022. https://archive.bahria.edu.pk/buic/law/wp-content/uploads/2024/05/Article-2-of-2022.pdf.

Blackstone School of Law & Business. "Digital Evidence and the Administration of Criminal Justice." Blackstone School of Law & Business. Accessed September 2026. https://www.bsolpk.org/digital-evidence-and-the-administration-of-criminal-justice.

City Laws. "PECA Act 2025: DRPA Powers & Cybercrime Penalties Guide." CityLaws.pk, April 5, 2026. https://citylaws.pk/prevention-of-electronic-crimes-amendment-act-2025/.

Dawn. "Punjab Police File Three Cases under PECA for Deepfake Content." Dawn, February 21, 2025. https://www.dawn.com/news/1893349.

Farooq, Muhammad Umar, Ali Javed, Khalid Mahmood Malik, and Muhammad Anas Raza. "A Lightweight and Interpretable Deepfakes Detection Framework." arXiv preprint, 2025. https://arxiv.org/pdf/2501.11927.

Human Rights Watch. "Pakistan: Repeal Amendment to Draconian Cyber Law." Human Rights Watch, February 3, 2025. https://www.hrw.org/news/2025/02/03/pakistan-repeal-amendment-draconian-cyber-law.

International Federation of Journalists. "Pakistan: PECA Amendments Further Tighten Government Grip on Digital Expression." IFJ, January 29, 2025. https://www.ifj.org/media-centre/news/detail/article/pakistan-peca-amendments-further-tighten-government-grip-on-digital-expression.

International Media Support. "In Pakistan, Cyber Law Amendment Criminalises Disinformation, Tightens Control on Digital Expression." IMS, March 5, 2025. https://www.mediasupport.org/blogpost/pakistani-journalists-protest-peca-amendment/.

Journal of Development and Social Sciences. "Digital Evidence and Its Admissibility under Pakistani Law." Journal of Development and Social Sciences. Accessed September 2026. https://ojs.jdss.org.pk/journal/article/download/67/164/297.

Kasuri, Ahmad Ali. "Lecture on Use of Modern Devices and Techniques for Evidence as Envisaged in Article 164, Qanun-e-Shahadat Order 1984." SlideShare, April 25, 2019. https://www.slideshare.net/slideshow/lecture-on-use-of-modern-devices-and-techniques-for-evidence-as-envisaged-in-article164-qanun-shahadat-order1984-pakistan/142155426.

Nasir Law Site. "The Qanun-e-Shahadat Order, 1984 (10 of 1984)." Nasirlawsite.com, May 25, 2016. http://nasirlawsite.com/laws/evidence.htm.

Record of Law. "The Misuse of Deepfake Technology: Addressing the Legal Gap in Pakistani Law." Record of Law, 2026. https://recordoflaw.in/the-misuse-of-deep-fake-technology-addressing-the-legal-gap-in-pakistani-law/.

Recording Law. "Pakistan Recording Laws: Consent, PECA 2025, and Penalties (2026)." RecordingLaw.com, May 15, 2026. https://www.recordinglaw.com/world-laws/world-recording-laws/pakistan-recording-laws/.

SAHSOL (LUMS Law Journal). "Deepfakes and Digital Identity: What Pakistan Can Learn from Denmark's Deepfake Law." SAHSOL, February 18, 2026. https://sahsol.lums.edu.pk/node/27600.

Sarhad Journal of Legal Studies. "AI-Generated Deepfakes and the Crisis of Legal Authenticity: Reconstructing Evidentiary Standards in the Digital Age." Sarhad Journal of Legal Studies, January 31, 2025. https://journal.suit.edu.pk/index.php/sjls/article/view/1126.

Umar, Muhammad. "Deepfake Cyberlaw in Pakistan." TILS Law Review, September 2025. https://tils.edu.pk/wp-content/uploads/2025/09/Muhammad-Umar-Deepfake-Cyberlaw.html.

IEEE Institute for Excellence in Education & Research

VOA News. "Pakistani Journalists Fear Amended Cybercrime Law Will Further Curb Freedoms." Voice of America, January 30, 2025. https://www.voanews.com/a/pakistani-journalists-fear-amended-cybercrime-law-will-further-curb-freedoms-/7952337.html.

IEER
Institute for Excellence in Education & Research