UCP Journal *of* Law & Legal Education
Vol. 3, Issue 3 (July – December 2025)

Admissibility of Artificial Intelligence-Based Evidence in Pakistan: Legal Standards and Judicial Responses

Bisma Javaid*, Shehryar Saleem*

Abstract

Integrating Artificial Intelligence (AI) in the judicial system has introduced transformative possibilities, particularly in evidence generation and analysis. This paper critically examines the admissibility and legal standards of AI-based evidence in Pakistani courts, employing the doctrinal research methodology. The study systematically analyses primary and secondary legal sources, including the Qanun-e-Shahadat Order, 1984, statutory provisions, judicial precedents, and scholarly interpretations, to evaluate how Pakistan's legal framework accommodates AI-based evidence. The research identifies gaps in existing laws regarding the principles of reliability, authenticity, and relevance when dealing with AI-based evidence. The study also investigates the challenges posed by algorithmic biases, lack of transparency in AI processes, and technical complexities, which can hinder the fair evaluation of such evidence. Furthermore, analysis of global best practices such as those in the United States, the United Kingdom, etc., highlights the need for specific legislative and procedural reforms in Pakistan. The findings show how AI may hold great potential for improvement in evidence accuracy and efficiency, but that the Pakistani judiciary needs specific guidelines on its admissibility and value. The paper presents recommendations for the adoption of best practices, including AI literacy and judicial training, on requisite safeguards against its misuse for protecting due process rights. Hence, this paper contributes to the discourse on AI and law by advocating for a balanced approach that embraces technological innovations while safeguarding judicial integrity and due process in Pakistan.

* Assistant Legal Manager, Northmen & Sterling, Rawalpindi, Pakistan. Email: bismajvd1998@gmail.com
** Lecturer, Government Degree College, Peshawar, Pakistan. Email: sherysaleem1@gmail.com

Article History: Received: 16-11-2025; Received in revised form: 28-05-2026; Accepted:02-06-2026.
Available online: 08-06-2026
DOI: https://doi.org/10.24312/ucp-jlle.03.03.739

Keywords: *Artificial Intelligence, Admissibility, Digital Evidence, Judicial Standards, Legal Framework, Ethical Challenges*

Introduction

Artificial Intelligence (AI) is massively changing the legal environment across the world and redefining the functions of courts, the process of evidence, and the administration of justice. With AI-based tools playing an increasingly important role in the judicial process, there is both an opportunity and a threat to the judicial process. AI-based evidence, such as forensic facts, crime-prediction algorithms, and deepfakes, is increasingly being used in legal settings (Hashmi, 2025). Nonetheless, the admissibility of this evidence is controversial as multiple issues of reliability, authenticity, transparency, and ethical considerations arise. The current judiciary system of Pakistan, owing to the Qanun-e-Shahadat Order 1984, has no explicit provisions relating to AI-based evidence, and thus legal changes are necessary to adapt to such technological changes.

In various jurisdictions globally, AI has been integrated into the justice system in automated legal research, AI-based forensic software, verification of digital evidence, and predictive analytics (Grimm et. al., 2021). These AI sensors help analyse documents, detect faces, assess risk, and carry out digital forensics, making them more accurate and efficient in court. In the United States, risk assessment systems founded on AI are built to inform sentencing, and in the European Union, AI-based legal analytics predict case outcomes (White, 2024).

In Pakistan, the Prevention of Electronic Crimes Act (PECA) of 2016 regulates the use of digital evidence, despite the lack of any specific legal provisions concerning AI-based evidence or its admissibility in courts. The National Artificial Intelligence Policy seeks to integrate AI in every sector, including the judicial system, by responsibly and ethically adopting AI (Akhtar, 2025). However, without clear statutory guidelines, AI-based evidence is always vulnerable to judicial challenge and to data tampering, bias, and interpretability.

The major issues regarding AI-based evidence are as follows:

Reliability and Bias: AI algorithms can make biased predictions based on historical data used to train them, which can be discriminatory (Angwin et al., 2016). Before admitting AI tools as evidence, courts have to determine whether they are reliable and unbiased.

Transparency and the Black Box Problem: Most AIs have a black-box nature, which does not guarantee explainability in their reasoning (Zarsky, 2016). This obscurity obstructs the certification of AI-produced forensic evidence.

Legal and Ethical Issues: The possibility of manipulating AI-based evidence, including deepfakes, is highly controversial. Courts must establish measures to avert abuse of AI technologies in court (Chesney & Citron, 2019).

Lack of a Parliamentary Framework: The Qanun-e-Shahadat Order of 1984 does not explicitly cover the evidence created by AI, so its admissibility can be doubted. Current legal requirements should be modified to include the use of AI-based forensic software, such as machine-learned predictions, and computerised evidence validation.

This issue regarding the admissibility of AI-based evidence in Pakistani courts has now become urgent. The key research question, which addresses the general principles of AI-based evidence admissibility in Pakistan and its correspondence with international best practices, is further divided into the following research questions: (1) How do existing legal standards facilitate AI-based evidence in court proceedings? (2) What are the legal and ethical issues that are raised by the use of AI-based evidence? (3) What adjustments need to be made for the incorporation of AI-based evidence in the Pakistani legal system?

Research Methodology

This study uses doctrinal research methodology, which implies the examination of legal doctrine, laws, case law, and judicial precedent relating to the admissibility of evidence generated by AI. The research examines the Qanun-e-Shahadat Order of 1984 and other Pakistani laws relevant to the admissibility of evidence in digital technology. In Pakistan, the primary sources of legislation governing the admissibility of evidence involve statutory law, judicial law, and constitutional principles. The main statutory text, the Qanun-e-Shahadat Order of 1984, is thoroughly examined to ascertain the extent to which it can be applied to AI-based evidence. PECA of 2016 is also analysed as a potential legislative measure on digital evidence. The legal materials were engaged through a qualitative doctrinal analysis, whereby each statutory provision was interpreted textually and purposively to determine its scope of application to AI-based evidence. International case laws are studied to comprehend how different courts have reasoned through questions of digital and AI-based evidence, and whether such reasoning can be transplanted in Pakistan. Where applicable, legislative documents such as the Qanun-e-Shahadat Order, 1984, and PECA 2016 were evaluated not merely for their existing provisions but also for their interpretive gaps, thereby enabling a constructive critique of the existing legal framework. This multi-layered doctrinal engagement, combining textual analysis, comparative jurisprudence, and case-law review, strengthens the methodological foundation of the study and enhances its capacity to generate actionable legal recommendations (McKeon, 2020).

Secondary materials include academic articles, textbooks, research papers, policy documents, and international legal frameworks that are discussed in AI-based evidence processing across jurisdictions. One essential element of this study is comparative legal analysis, which evaluates how developed law systems, including those of the US and UK, have implemented AI-based evidence.

The research examines whether jurisdictions possessing well-developed legal systems addressing AI evidence have put in place some definite criteria as to the admissibility, reliability, and

authenticity of artificial evidence, and whether Pakistan can replicate similar approaches through legislative action. It also examines judicial case law in Pakistan and cases from other countries to determine how courts are inclined to accept digitally based evidence. Since the AI evidence in specific Pakistani case law is limited, the study reviews relevant foreign court decisions where AI-generated forensic reporting, forecasts of crime patterns, or digital AI software were pleaded or contested at trial. The study of such cases can yield useful information towards reforms that Pakistan should make in its laws. This paper has used the policy implications of the National AI Policy of Pakistan as a means to examine how AI can be applied in the judicial sector under both ethical and legal paradigms. It also analyses the global regulatory policies and industry forward-looking practices concerning AI governance, forensic AI, and the management of digital evidence. The research follows a doctrinal approach and will aim to carry out an extensive legal overview of the issues that are related to AI-based evidence in Pakistan.

The research will complement the existing legal literature by locating loopholes, suggesting reform of the law, and making suggestions for judicial best practices for ensuring proper and effective use of AI-based evidence in Pakistani courts.

Literature Review

The use of AI has significantly changed the process of judicial proceedings, including the process of obtaining, checking, and admitting evidence. With the increased acceptance and usage of AI-based evidence among the public, the question of its admissibility, visibility, and impartiality remains the epicentre of the existing legal discussions. This section critically reviews literature on AI evidence, follows its evolution, highlights important issues, and raises questions of ethics and the need for reforming the laws.

It is observed that the application of AI in the judicial process has significantly increased within the last ten years. Grimm et al. (2021) argue that legal AI technology, which involves the use of AI in forensic data analysis, computer-assisted review of documents, and predictive modelling, has radically transformed the

process of evidence consideration in the courts. The technologies have made judicial procedures easier due to the backlog of cases, the minimisation of errors, and the provision of up-to-date data in the course of proceedings. Also, AI is increasingly used in predictive policing, crime forecasting, and forensic analytics to identify criminal trends and to automate crime investigation (Berk, R. A. 2021).

According to Ahmed et al. (2024), a growing dependency on AI-based decision-making software is observed in the European legal system. The European Union has, in turn, responded by setting up regulatory standards to ensure the AI-enabled legal tools are transparent, responsible, and fair. Likewise, in the United States, AI-based risk-assessment tools are used in the sentencing process to help judges assess the likelihood of recidivism based on past case information (White, 2024).

However, the introduction of AI in courts has not been smooth sailing, with issues of interpretability and accountability. Researchers believe that the black-box nature of AI makes it difficult for the judicial community to assess the credibility and reasonableness of AI-generated rulings (Zarsky, 2016). This is a debate as to whether AI-created evidence meets the necessary criteria of authenticity and reliability in the court of law, because of its opaque nature. Admissibility of AI-generated evidence is a controversial matter with numerous arguments, the main ones being authenticity, reliability, and bias. According to Hameed et. al. (2021), AI-generated evidence must satisfy the traditional relevance, authenticity, and chain of custody tests. However, AI technology is based on algorithmic frameworks that can be closed, and the soundness of such an algorithm in a court of law is debatable.

The most significant problem with the evidence of AI is arguably algorithmic bias. The machine-learning algorithms that are trained using past information are bound to have some inherent discrimination, consequently making AI predictions discriminatory. In a study on the COMPAS risk-scoring tool, Angwin et al. (2016) discovered that the tool was more likely to award high scores on recidivism to Black individuals as opposed to White defendants.

Such biases highlight the dangers of using AI evidence without trying to make it objective.

The black-box issue is one of the real issues that demonstrates the lack of transparency in the AI decision-making processes. According to Zarsky (2016), AI models use sophisticated algorithms, which make it impossible for legal experts to understand the ways in which particular results are obtained. Lack of explainability can cause AI-based evidence to fail to meet the high-quality criterion of expert testimony in many jurisdictions, such as the Daubert Standard in the US (Faigman et al., 2017).

Even though AI-based evidence is currently gaining recognition in the legal system, there is no standardised legal system to determine the admissibility of this evidence. According to Ahmed et al. (2024), the use of regulatory tools like the AI Act has been enacted in the European Union to regulate the use of AI in the judiciary. Such rules are created to permit transparency, fairness, and accountability regarding AI-generated evidence.

On the other hand, the legal system in Pakistan does not specifically deal with AI-based evidence. The emphasis by the Qanun-e-Shahadat Order, 1984, and the PECA, 2016, is mostly based on digital evidence, whereas AI-predicted forensic tools are absent (Hameed et al., 2021). Therefore, courts in Pakistan still use classical evidence-evaluation principles that might be insufficient in addressing the challenges posed by AI. Even the fact that AI-based evidence has no judicial precedents that can be cited to further support its admissibility in Pakistani courts suffices to suppress its introduction into the country.

White (2024) addresses the history of the creation of the U.S. court standards for testing AI-based evidence. The Daubert Standard is usually used to evaluate the admissibility of expert scientific evidence, and this must have a consistent process, peer review, and an error rate.

The legal implications of AI evidence have started gaining importance due to ethical issues related to AI. Grimm et al. (2021) underscore the fact that biased training data has discriminatory

consequences, especially in criminal adjudications. Biased datasets can further promote social prejudice, hence compromising the right to a fair trial.

Moreover, there is also a strong ethical concern about deep-faked evidence manipulation. The development of AI has enabled the creation of highly realistic artificial video clips, voice recordings, and textual data that can be used to fabricate evidence (Chesney and Citron, 2019). Judges should thus employ effective forensic verification methods to identify AI-generated evidence and distinguish it from genuine evidence.

Considering the complexities influencing the AI evidence on the matter, researchers emphasise the need to initiate substantial changes in legislation. Ahmed et al. (2024) encourage the application of AI to particular legal norms in Pakistan, comparable with those launched by the EU and the US. These criteria must foster clarity, reduce bias, and offer clear rules on expert witness testimony with regard to AI evidence.

To guarantee the Enforcement of AI ethics in Pakistani laws, Hameed et al. (2021) suggest proposing legislative reforms when it comes to the application of AI in court. Moreover, the successful implementation cannot be achieved without the education of judges, lawyers, and forensic experts in AI literacy. The AI-related issues that require legislative adjustments include the accountability of AI-related mistakes, the regulatory framework, and the liability system in case AI evidence substantially affects the verdict of the court proceedings.

Legal Regime relating to Evidence in Pakistan

Qanun-e-Shahadat Order, 1984, is the most significant legal code that governs the evidence in Pakistan. It provides the vital provisions that touch on admissibility, authenticity, and relevancy of the evidence given in the courtroom. There are three types of evidence: documentary, oral, and electronic, which are subjected to different authentication processes. However, AI-based evidence does not fit easily into these accepted classes, thus posing a conflict about how it can be classified and whether it is admissible. Although

courts have accepted electronically stored information (ESI) as digital forensic evidence, the requirements of procedural and evidentiary standards for AI-generated data have not been sufficiently established. In turn, the absence of direct legal provisions related to AI evidence requires reforms to be made, which include technological advancements in the judicial system (Hameed et al., 2021).

The Prevention of Electronic Crimes Act, 2016, talks about the reception of electronic evidence, the investigation of cybercrime, and the methods involved in digital forensics. However, PECA does not impose the requirement to include the information created by AI, which assumes that it is not binding in a court of law. It is important to draw a clear distinction here: while PECA 2016 addresses digital evidence broadly, covering electronic records, cybercrime investigations, and forensic data. However, it does not contemplate AI-based evidence as a distinct evidentiary category. This distinction is critical. PECA was legislated in an era when AI-driven forensic tools had not yet entered mainstream legal proceedings in Pakistan. Consequently, evidence produced by machine-learning models, predictive policing algorithms, or autonomous forensic AI systems falls outside PECA's explicit regulatory purview, leaving a significant statutory gap (Hameed et al., 2021).

The National Artificial Intelligence Policy (2023) recognises the potential role of AI in improving governance and public-sector systems, including areas relevant to judicial modernisation. However, as a policy instrument rather than binding legislation, it does not itself establish enforceable obligations or a specific evidentiary framework for the admission of AI-generated evidence. Pakistan's future AI regulation should also consider international developments in cybercrime, data protection, and AI governance frameworks to ensure compatibility with emerging global standards.

Existing legal frameworks are not adequately aligned with the distinctive characteristics of AI-generated evidence. Although the PECA 2016 recognises electronic evidence, it does not suggest any specific admissibility grounds for AI-based forensic analysis in Pakistani law. It follows that the legislature needs to come up with

clear provisions about the admissibility of AI-based evidence in the Qanun-e-Shahadat Order to bring it more in line with international law. Regarding the emergence of deepfakes, AI-generated text and the forensic use of AI, the judiciary must develop a set of standards about the authenticity, reliability, and relevance of AI evidence (Grimm et al., 2021). The amendments to the legislation should include a standard procedure of forensic verification, the regulation of AI ethics, trainings for the successful use of AI-generated evidence.

The rulings of the Pakistani courts regarding electronic and digital evidence have established some principles regarding data integrity, forensic authentication, and the chain of custody. At the moment, no judicial precedents apply to AI-based evidence in Pakistan. However, international jurisprudence, such as rulings on AI-based forensic evidence, e.g., facial-recognition reports and predictive policing algorithms, can be helpful to guide Pakistani courts.

Scientific validity, peer review, and transparency of AI decision-making should be ensured prior to the admissibility of AI evidence in court. U.S. courts' rulings can help shape an idea about the best practices in incorporating AI-based evidence into the legal system of Pakistan (Ahmed et al., 2024).

Principles of Admissibility of AI-Based Evidence

Reliability: Accuracy of Outputs from AI

Legal cases will largely depend on the reliability of evidence obtained through AI. AI systems are based on machine-learning models that are trained using large amounts of data; hence, they should be as dependable as the quality of the data, training, and systemic uniformity. The judges must provide guidelines under which AI-based evidence is treated more strictly, such that the tools employed in forensic and legal analysis yield the same quality of evidence as traditional evidence (Grimm et al., 2021).

The judicial use of internationally recognised norms, including the Daubert Standard, or expert testimony on testability,

review by peers, known falsehood rates, and general acceptance by the scientific community, and the Frye Standard, or the requirement that the scientific methodology be accepted by its discipline, can also be introduced to AI-derived forensic evidence (Fairfield, 2026). The adoption of such standards will ensure that AI evidence is seriously vetted and verified before admissibility.

Furthermore, it is recommended by law specialists that independent third-party tests and expert witnesses should be included. Since AI systems are technologically advanced, forensic experts are expected to give clear answers about the derivation of conclusions. The presence of AI certification programs would also guarantee that the forensic tools are certified before they are presented in court (Cihon et al., 2021)

Authenticity: Authentication of the Source and Process of AI Evidence

Authentication is one of the principles for confirming the authenticity of AI-based evidence. This evidence should be able to show its origin, and a system of controls should be put in place to ensure the verifiability and safety of processes involved in its formation (Ahmed et al., 2024). Lack of sound authentication measures exposes AI-based evidence to hacking, corruption, and bias.

A valid solution is blockchain technology, which can provide evidence chains and immutable digital transactions. Authentication based on blockchain may allow courts to trace the authenticity of AI-generated data and ensure that it is impossible to modify it once created (Casino et al., 2019). Moreover, the forensic AI tools should include audit logs regarding all the data processing and transformation steps undertaken by the AI models during their developmental stages. Strict chain-of-custody measures would support evidence based on AI and would improve the authentication of such evidence. The AI forensic experts should keep a detailed log of all aspects of AI's data collection, processing, and analysis. By doing so, they would make sure that no unauthorised changes have been made to the respective AI model.

Relevance: Considering AI-Based Evidence within Judicial Hearings

For the AI-based evidence to be admissible before the court, it should be directly related to the legal substance of the case. The judiciary should question the contribution to the case by that evidence which is of any meaningful contributory effect, and determine whether the value of the information is probative over any prejudicial effect. The main issue is that legal professionals and judges should be knowledgeable enough when it comes to AI-generated evidence and factors like that to be able to rate whether it is appropriate. The outputs of AI are, by their nature, probabilistic; they are not absolutely true assertions, but probabilistic estimates using statistics (Surden, 2019). The judges have to answer the question as to whether these types of probabilistic outcomes can be politely considered legally admissible or whether they fall under the category of inappropriate speculation in judicial reasoning.

The other essential area is the compatibility of AI-generated pieces of evidence with conventional methods used in forensics. The use of AI findings should not be overly accepted in courts where conventional methods of evidence gathering have not been able to support them. This would help to eliminate the risk of AI errors exerting an overbearing influence on court rulings.

Challenges in Admissibility of AI-Based Evidence

Algorithmic Biases: Impact on Fairness

The bias in the fairness of AI systems can easily permeate into legal procedures. Prejudice results when AI models are trained on a welter of historical injustices. Such a result of the training is unfair or biased. AI-based evidence bias is very difficult for criminal processes, in which predictive policing instruments and forensic AI algorithms have been put in place to target disadvantaged classes disproportionately (Grimm et al., 2021).

To solve the problem of algorithmic bias, the disclosure of training data and methodological information that is used in AI systems should be presented in court. Providers of training, validation, and certification of AI models should provide transparent

documentation in the form of reports provided by the developers and forensic auditors. The use of AI systems in litigation can also be further monitored through independent oversight bodies that perform a bias audit to verify the compliance of the systems with set fairness standards (NIST, 2023). Within the specific context of Pakistan's judicial system, these mitigation strategies require institutional grounding. The Federal Investigation Agency (FIA) and provincial forensic laboratories currently lack a standardised protocol for auditing AI-based forensic tools before they are admitted into evidence. A practical first step would be the creation of an independent AI Audit Commission, operating under the Ministry of Law and Justice, tasked with certifying AI tools used in criminal proceedings for fairness, accuracy, and methodological soundness. Drawing on the model of the National Institute of Standards and Technology (NIST) AI Risk Management Framework in the US, such a body could develop context-specific fairness benchmarks calibrated to Pakistan's demographic and socio-legal conditions (NIST, 2023). Additionally, mandatory third-party algorithmic impact assessments, conducted before any AI forensic tool is deployed in a Pakistani court, would provide a structured mechanism to detect and correct bias before the admission of evidence.

Lack of Transparency in AI Processes

The black box problem, or the lack of understanding of how AI decision-making works, is a significant obstacle to the admissibility of AI-based evidence (Ahmed et al., 2024). The technological depth of most AI algorithms interferes with the ability to explain them in words, making it difficult for the judge to evaluate the AI's conclusions. As a result, the forensic findings obtained by AI can be questioned. To overcome this problem, the law should set the requirement for explainability and interpretability when the AI system is used in forensic analysis. The creators of artificial intelligence should model systems that produce clear and understandable descriptions of analysis processes. Courts also need to demand that AI verdict presentation be followed by expert testimony that puts such conclusions in a practical and interpretative context comprehensible to legal professionals. Two parallel solutions are worth considering when it comes to the black box issue

in Pakistan's judicial dealings. A Court-Appointed AI Expert Panel composed of professionally trained data scientists, forensic technologists, and legally qualified digital experts would serve as a permanent interpreting panel to which parties could appeal decisions generated by AI systems. These panels would serve as a middle ground to help understand the difference between the technical aspects of AI-generated content and the legal standards that courts are expected to adhere to. Secondly, Pakistan might require the implementation of "explainable AI" (XAI) models in any AI applications used in criminal and civil cases. Explainable AI systems can give the judge both a result and a rationale, which provides insight into the way in which the algorithm reached its decision, allowing the judge to evaluate the results as well as the reasoning (Chaudhary, 2024). This direction has already been taken by several jurisdictions, such as in the United Kingdom via the UK Algorithmic Transparency Recording Standard, which could be implemented in Pakistan either via proposed amendments to PECA 2016 or through a stand-alone AI Evidence Regulation Act.

Technical Sophistications in Understanding AI Systems

The data generated by AI is often very technical and cannot be understood by legal experts. Attorneys, prosecutors, and judges might be lacking the necessary expertise to cast a critical analysis on AI-based forensic tools (White, 2024). A knowledge gap should be addressed by creating special training units of legal professionals. Introducing AI consultative councils of forensic specialists in courts would help in the examination of AI-driven evidence. To prepare law school graduates to be competent in the future of AI and law, AI ethics, digital forensics, and machine learning should be taught in legal education programs.

Potential Misuse and Ethical Issues

Evidence created by AI presents the dangers of manipulation, deepfakes, and moral abuse in courts. False evidence may be produced using deepfake videos and fake AI data, which can result in an incorrect conviction (Hameed et al., 2021). To manage the authenticity of AI evidence in courts, measures should be established that help detect and discourage the use of fabricated

evidence. AI experts' involvement in verifying evidence is a crucial protective measure that needs to be emphasised in Pakistan's legal system. When serving as an impartial court expert, a qualified AI specialist may deliver an objective, technically valid evaluation of whether a piece of AI evidence has been manipulated, fabricated, or processed in a way that is not in keeping with its purported source. The definition of AI scientists and digital forensic technologists who are competent in machine-learning systems is not currently included in the definition of "expert" as provided under Article 59 of the Qanun-e-Shahadat Order, 1984. This change would recognise the expertise of the AI community and provide a mechanism for structured and accountable verification of deepfakes and other types of AI-manipulated information (Maddox, 2024). Furthermore, the court might mandate that the AI evidence each party presents be vetted by a court-registered AI expert before its admission, which would help maintain fairness and evidentiary integrity at the admission stage.

Potential solutions are the creation of forensic AI verification tools that can help to differentiate between original and synthetic AI-generated evidence, and the establishment of strict admissibility rules that would be enforced on AI-based evidence and which would involve cross-verified AI evidence based on traditional forensic techniques.

There must also be set ethical rules to make sure that AI evidence will not contradict the idea of fairness, due process, and human rights. Comparable oversight bodies need to devise supervisory systems that would eliminate AI misuse in courts and ensure that humans are not subjected to unfair AI-related rulings.

Global Best Practices

United States of America (USA)

The US has developed a procedural legal system for AI-generated evidence in legal cases. To measure such evidence in terms of its reliability and authentication, the Federal Rules of Evidence (FRE) are the standard point of reference. Scientific reliability must be present under Rule 702 to support AI evidence,

whereas Rule 901 demands that such proof must be authenticated first before admission. The proposed Artificial Intelligence Act (AIA) aims to provide some sort of accountability in the use of AI during court proceedings, hence making sure that there is transparency and justice in the fulfilment of decisions that are based on AI analyses (Grimm et al., 2021). This trend is evidence of an increased realisation of the need to reconcile the advancement of technologies and the protection of due process (Gless et al., 2024).

Regulatory authorities are another factor that can contribute to the development of AI evidence governance, other than the legislatures. The National Institute of Standards and Technology (NIST) published the AI Risk Management Framework that provides the courts with guidelines to determine the reliability of the evidence presented by AI. Though useful, these frameworks are not statutory, which may lead to variation in courts' determination of AI reliability (Gless et al., 2024). The aspect of transparency and accountability is something that judges should weigh, especially in cases when the proprietary algorithms do not allow the inspection of their decision-making process (Grimm et al., 2021). There must be procedural protections so that the AI-generated evidence can fit the minimum legal standards (Gless et al., 2024).

State v. Loomis (2016) is one of the classic instances of legal cases related to AI-generated evidence. The secrecy of the AI algorithm, used to sentence with regard to risk assessment, also contributed to a due-process concern because judicial openness was undermined by the fact that the algorithm that guided the decision-making process was not auditable. The court permitted AI-assisted evaluation but demanded greater transparency and accountability in AI-based judicial decision-making. The case is also a pillar in the discussion of the increased regulation and research on the ethical form of AI use in the judicial process (Gless et al., 2024). However, it is important to note that even the well-established Daubert Standard has faced growing criticism in its application to AI-generated evidence. Scholars have pointed out that the Daubert criteria, originally designed to assess conventional scientific testimony such as DNA evidence or medical expert opinion, were not conceived with algorithmic or machine-learning processes in mind. For instance, the requirement that a methodology be

"testable" and have a "known error rate" is difficult to apply to proprietary AI systems whose inner workings remain opaque, even to their developers (Faigman et al., 2017). Critics further argue that Daubert's reliance on peer review and general acceptance in the relevant scientific community is undermined in the AI context, where rapid technological development outpaces academic scrutiny, and there is no settled "scientific community" for many cutting-edge AI forensic tools (Grimm et al., 2021). These limitations illustrate that even the most sophisticated legal systems are still grappling with how to reconcile traditional evidentiary standards with the novel challenges posed by AI, a realisation that should inform Pakistan's legislative approach as it builds its own framework from the ground up.

United Kingdom (UK), European Union (EU) and Canada

The UK has developed principles governing the admissibility of AI-generated evidence in legal proceedings. Judicial assurance through independent checking of AI-generated outcomes is developed in the Criminal Procedure Rules (CPR 35) and the Civil Procedure Rules (2023) (Gless et al., 2024). The Artificial Intelligence (Regulation) Bill (2023) also establishes a mechanism for decision-making under AI in court (Grimm et al., 2021). The current court standards emphasise that, although AI software can be used in court, it is only judges and lawyers who are responsible for ensuring that AI-generated information can be deemed reliable and accurate. The implementation of human control should be kept as a vital measure, especially when legal cases are involved at a high level.

Artificial intelligence systems used in courts have been designated as high-risk by the European Union in the Artificial Intelligence Act (2024) and must be strictly regulated according to Article 10 (governance of data) and Article 14 (human oversight). Article 22 is another piece of evidence of due process in the General Data Protection Regulation (GDPR), according to which no automated decision-making should be made in the absence of real human involvement (Ahmed et al., 2024). These regulations ensure fairness, transparency, and accountability of the judicial decisions made by AI (Gless et al., 2024).

The use of regulations with regard to evidence in Canadian law has been realised through the Canada Evidence Act (Sections 31.1–31.8) in harmonising the authentication process of evidence obtained as a result of AI. The Personal Information Protection and Electronic Documents Act (PIPEDA) encourages transparency as it makes judicial decisions influenced by AI subject to human review. All these legislative and legal actions also show what Canada is doing to ensure that AI technology integration in the laws takes place in a responsible manner.

Best Practices: Lessons for Pakistan

Pakistan has recognised the development of international jurisdictions and is now set to introduce AI evidence laws in line with international best practices (Sahar G., 2026). The Qanun-e-Shahadat Order of 1984 does not explicitly refer to AI, and the PECA does not mention AI-based digital evidence. In the modern world, judicial tradition, based on traditional admissibility tests, could be insufficient to deal with the peculiarities of AI-based evidence (Hameed et al., 2021).

Pakistan can emulate ideal examples in order to fill this gap. It would be a good move to revise the Qanun-e-Shahadat Order 1984 to include provisions for AI-generated evidence in line with the Canada Evidence Act, 1985. Implementing transparency standards akin to the UK Criminal Procedure Rules (CPR 35) would ensure that there is disclosure of artificial intelligence decision-making. Judicial training on AI-based case design on the lines of the NIST AI Risk Management Framework (U.S.) would increase the ability of judges to examine AI-generated evidence critically. The creation of an autonomous AI audit agency will be responsible and reliable when it comes to AI in the court. Moreover, it would be beneficial to draft an AI and Evidence Regulation Act, based on the details of the EU AI Act (2024), to offer Pakistan an effective legislative system to regulate AI-generated evidence.

Fortunately, Pakistan has already taken certain steps towards this direction. The Ministry of Law and Justice (2024) contemplates in earnest an AI regulation bill comprising provisions that could entail a lot of legal implications. Monitoring international trends and

implementing specific reforms can help Pakistan have a progressive legal system that will make the AI-generated evidence admissible, credible, and fair during court hearings (Hameed, Qaiser, and Qaiser, 2021).

Recommendations for Legal and Procedural Reforms in Pakistan

Drafting Specific Legislative Guidelines for AI-Based Evidence

Proposed Amendments to the Existing Articles of Qanun-e-Shahadat Order, 1984

Table 1

Proposed Amendments to the Existing Articles of Qanun-e-Shahadat Order, 1984

Existing Articles of QSO 1984	Amendment Needed
Article 46 (Presumption under Documents in Electronic Form)	Mention the scope specifically to admit AI-generated documents and electronic records as permissible evidence, bearing the reliability and authenticity standards (Seng & Mason, 2021).
Article 59 (Expert Testimony on AI-Generated Evidence)	Amend the definition of "expert" to include artificial intelligence, data science, and digital forensics experts to provide courts with qualified persons' testimony on creating AI-generated evidence (Seng & Mason, 2021).
Article 59-A (Validation of AI-Generated Evidence)	Add a new article mandating that AI-based evidence be validated by expert opinion and comprehensive technical verification to ensure fairness and transparency.
Article 73 (Digital and AI-Generated Record Evidence)	Employ AI-generated records as direct evidence only with forensic authentication to avoid having courts make judgments on tampered or biased AI results (Maddox, 2024).
Article 78 (Authentication of Digital Records Generated by AI)	Enact forensic verification and metadata analysis of digital records created by AI to verify and safeguard against tampering (Emehin et. al., 2024).

Article 129 (Presumption of Fact on AI Evidence)	Create a legal presumption that AI-based evidence is not reliable unless separately authenticated, to avoid algorithmic bias and manipulation risks (Seng & Mason, 2021).
Article 153 (Challenging AI-Generated Evidence and Witnesses)	Grant plaintiffs the right to impeach AI-based evidence because of data manipulation, bias, and inadequate disclosure of algorithms to ensure due process (de la Osa & Remolina, 2024).
Article 157 (Examination of AI Experts)	Require experts to introduce AI-based evidence to reveal technical information, such as algorithmic design, data sources, and measures for avoiding bias, so that courts may examine the authenticity of AI systems (de la Osa & Remolina, 2024).
Article 164 (Courts' Discretion to Accept AI Evidence)	Empower courts to accept AI-based evidence only on the grounds of independent audit reports, algorithm validation, and technical transparency, providing an assurance of fairness in court proceedings (Balakrishnan, 2024).

Preparing Specific Legislative Rules for AI-Based Evidence

In order to guarantee the admissibility and reliability of AI evidence in the Pakistani judicial framework, specific legislative recommendations are necessary. The laws must outline explicit legal guidelines in the evaluation of reliability, authenticity, and admissibility, and also prescribe technical requirements. It is suggested that the following provisions be provided:

Reliability Assessment

The laws must require a thorough test of AI tools used in legal proceedings in order to determine their accuracy, consistency, and reliability in various legal situations (Wachter et al., 2021). To promote judicial transparency and curb possible bias or manipulation, developers have to be compelled to release algorithmic architectures, training procedures, and decision-making processes (Chaudhary, 2024).

Data Provenance Documentation

Evidence generated by AI must be presented solely based on extensive records covering source data, pre-processing procedures,

and any calibrations to ensure evidentiary authenticity (Stoykova et. al., 2023).

Independent Audits

Laws must enforce independent third-party audits, and these audits must be done periodically to ensure judicial integrity and confirm that AI systems align with legal and ethical standards (de Almeida et al., 2021).

Chain of Custody Procedures

Certain legal measures should be put in place to ensure an unbroken, safe, and identifiable chain of custody of the AI-generated evidence to ensure that nothing is tampered with and that the integrity is not compromised (White, 2024).

Standardisation of AI Evidence Formats

The adoption of standard formats and documentation for AI-based evidence by the court must be worked upon by the legislature. This is necessary so that judicial review of AI-based evidence remains consistent across the board and the admissibility procedure becomes simplified (Stoykova, 2024).

Balancing Innovation and Judicial Integrity

Better efficiency, accuracy, and objectivity in the judicial process can be made possible by the application of AI in the courts. However, it poses important questions concerning the protection of due-process rights, the impartiality of the courts, and the unprejudiced assessment of the evidence provided by AI. This section discusses the usefulness of AI in the judiciary, the challenges that come with it, and the measures that should be put in place in order to ensure that innovation and judicial integrity comply with each other.

Judicial Neutrality and Protection of Due Process Rights

Regardless of the numerous advantages of AI, there should be safeguards to protect against the obliteration of core civil

libertarian principles like judicial non-partisanship and due process. Freedom of hearing and a fair hearing are fundamental rights of democracies in law. Introduction of AI-generated evidence should not compromise these rights and result in the development of prejudice, error, or uncertainty within the justice system (Drakokhrust & Martsenko, 2022).

One of the major weaknesses of AI-based evidence is algorithmic bias. The discrimination can only be as unbiased as the training data they are fed, because biased training data will replicate biased results. Research shows that AI cameras such as COMPAS have the ability to perpetuate racial and other socioeconomic prejudices, resulting in an unfair conviction (Grimm et al., 2021). The mechanisms of mitigation include the independent certification and strict verification of the AI systems to determine the absence of bias and adherence to the ethical standards.

Objectivity is another central test of the use of AI evidence in courts. Judges need to remain impartial and unbiased even when employing AI technology to assist their rulings. Judges have to be ready to possess a profound knowledge of the limitations of AI, and they should be able to critically assess the output of AI. The training programs must incorporate instructions on how to spot the moments when an AI output can be faulty or misguided to allow the judges to take the necessary precautions.

To enable the protection of rights of due process and judicial impartiality, carefully drafted application rules of AI have to be in the courts. The terms of such admission or non-admission should be properly mentioned, the principles of evaluating reliability must be formulated, and the measures to prevent bias or errors in judgment must be specified (Said et al., 2023). Also, they should train and constantly improve their knowledge in AI technologies to prepare judges to handle AI-based evidence's intricacies.

Ensuring Equitable Evaluation of AI-Based Evidence

Objective assessment of AI-based evidence requires a nuanced evaluation of its probative power and potential for misinterpretation or abuse. The evidence presented by AI is very

convincing but not always flawless, and therefore, the courts need to examine the genuineness and precision of the evidence produced by AI before it can be submitted in court. Such scrutiny includes an analysis of the algorithms and data input behind the evidence creation, combined with a venture into seeking possible prejudice or fallibility (White, 2024).

Among the ways of making sure that AI-based evidence has been evaluated objectively, one must refer to the practice of expert testimony employed to define the procedure and product of the AI system. As an example, accreditation to AI evidence under the Federal Rules of Evidence Rule 901, the person must personally present the evidence regarding those pieces of evidence that will determine that the AI-based evidence is authentic. Expert witnesses who are duly qualified specialists can explain how the AI system is designed, trained, and works (Grimm et. al., 2021).

Strategic implementation of procedural protections should be used to obtain an objective analysis of AI-based evidence. These protections would involve the obligatory publicity of the origin and procedures used by the AI framework, an adequate opportunity to object to it by the conflicting sides, and a review mechanism for the possibility of mistake or bias. As an example, the EU AI Act (2024) imposes the idea of high-risk AI systems being construed to determine whether high levels of both transparency and accountability are met when tested by third parties (European Commission, 2021).

Therefore, the incorporation of AI in the judicial system has immense benefits, such as increased accuracy, efficiency, and objectivity. However, it is a challenge to the right to due process, impartiality of the judiciary, and objective examination of evidence as well. Judicial independence and integrity must stay open-minded to encourage innovation, maintain procedural safety, and keep training judges and attorneys. By doing so, Pakistani authorities will be able to use AI to empower the country and promote legal regulations without jeopardising the principles of justice and equity.

Conclusion

For the legal system, AI has provided new opportunities in the areas of evidence generation and evidence analysis. The current legal framework of Pakistan, however, has yet to have in place the guidelines on the admissibility and evaluation of AI-based evidence. The legislation about the reliability, authenticity, and admissibility of evidence ought to be changed to deal with the specific vulnerabilities of AI, which include algorithmic bias, lack of transparency, and technical complications.

The paper proposes procedural and legislative changes so that Pakistan's legal system can keep up with AI-generated evidence. Based on best practices in other countries, it suggests solutions, including the development of AI literacy among the courts, the establishment of anti-abuse strategies, and the requirement that AI-based systems work according to the guiding principles of fairness and due process. All this is required to ensure the integrity of the judicial process by using AI to make the evidence more efficient and accurate. The recent development of generative AI, such as large language models generating extremely realistic synthetic text, deepfakes of audio-visual data, and/or AI-based forensic manipulation, is already jeopardising global judicial systems. The easy availability of digital and artificial intelligence-based technologies in the commercial, financial, and investigative fields has led to the increasing use of AI-generated documents in court proceedings, particularly in Pakistan, even without any specific legal framework. In this context, there is no neutral state of affairs, no lack of reform. There's a state of legal vulnerability.

While Pakistan follows the National Artificial Intelligence Policy (2023), which recognises the potential of AI in transforming various sectors, the judiciary has no specific binding instructions regarding the use of AI evidence (MoITT, 2025). The absence of legislative action is further widening the divide between the technological possibility of evidence creation by AI and the legal resources and tools needed to fairly assess it. The authors join others to make a call for prompt legislation, which should commence with specific amendments to the Qanun-e-Shahadat Order, 1984, and adoption of a separate AI Evidence Regulation Act based on

international best practices but sensitive to the local socio-legal context of Pakistan.

References

Ahmed, U., Fatima, Z., & Abbas, T. (2024). Implementing artificial intelligence (AI) into the judicial system in Europe: Challenges and opportunities. *Pakistan Social Sciences Review, 8*(1), 17–26. https://doi.org/10.35484/pssr.2024(8-I)02

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine bias: There's software used across the country to predict future criminals. And it's biased against Blacks. *ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Akhtar, H. (2025, December 15). https://issi.org.pk/issue-brief-on-pakistans-national-ai-policy-2025-developing-ai-ecosystem-and-ethical-data-governance/

Balakrishnan, A. (2024). *Ethical and Legal Implications of AI Judges: Balancing Efficiency and the Right to Fair Trial* (Master's thesis).

Berk, R. A. (2021). *Artificial intelligence, predictive policing, and risk assessment for law enforcement*. *Annual Review of Criminology, 4*, 209–237. https://doi.org/10.1146/annurev-criminol-051520-012342

Casino, Fran., Dasaklis, Thomas K., & Patsakis, Constantinos. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Chaudhary, G. (2024). Unveiling the black box: Bringing algorithmic transparency to AI. *Masaryk University Journal of Law and Technology*, *18*(1), 93–122.

Chesney, R., & Citron, D. K. (2019) Deep fakes: A looming challenge for privacy, democracy, and national security.

California Law Review, 107(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

Cihon, P., Kleinaltenkamp, M. J., Schuett, J., & Baum, S. D. (2021) AI certification: Advancing ethical practice by reducing information asymmetries. *AI and Ethics, 2*(2), 373–389. https://doi.org/10.1007/s43681-021-00072-6

De Almeida, P. G. R., dos Santos, C. D., & Farias, J. S. (2021). Artificial intelligence regulation: a framework for governance. *Ethics and Information Technology*, *23*(3), 505–525.

De la Osa, D. U. S., & Remolina, N. (2024). Artificial intelligence at the bench: Legal and ethical challenges of informing—or misinforming—judicial decision-making through generative AI. *Data & Policy*, *6*, e59.

Drakokhrust, T., & Martsenko, N. (2022). Artificial Intelligence in the Modern Judicial System. *J Mod Educ Res*, *1*.

Emehin, O., Emeteveke, I., Adeyeye, O. J., & Akanbi, I. (2024). Generative AI in forensic data analysis: Opportunities and ethical implications for cloud-based investigations. *International Journal of Research Publication and Reviews, 5*(10), 2941–2957.

European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* (COM/2021/206 final). EUR-Lex. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Faigman, D. L., Monahan, J., & Slobogin, C. (2017). Group to individual (G2i) inference in scientific expert testimony. *University of Chicago Law Review, 81*(2), 417–480.

Fairfield, J. (2026). The last human question: generative AI's existential threat to consensus and law. *The Research Repository @ WVU (West Virginia University)*. https://researchrepository.wvu.edu/wvlr/vol128/iss3/4

Gless, S., Lederer, F. I., & Weigend, T. (2024). AI-based evidence in criminal trials? *William & Mary Law School Scholarship Repository, Faculty Publications, Faculty and Deans*. Retrieved from: https://scholarship.law.wm.edu/facpubs/

Grimm, P. W., Grossman, M. R., & Cormack, G. V. (2021). Artificial intelligence as evidence. *Northwestern Journal of Technology and Intellectual Property, 19*(1), Article 2. https://scholarlycommons.law.northwestern.edu/njtip/vol19/iss1/2

Hameed U., Qaiser Z., & Qaiser K. (2021). Admissibility of digital evidence: A perspective of the Pakistani justice system. *Pakistan Social Sciences Review, 5*(4), 518–530.

Hashmi, H. (2025). Hajra Hashmi. Islamabad Policy Research Institute. https://ipripak.org/author/hajrahashmi/

Maddox, I. (2024). Artificial Intelligence in the Courtroom: Forensic Machines, Expert Witnesses, and the Confrontation Clause. *Case W. Res. JL Tech. & Internet*, *15*, 416.

McKeon, M. (2020). The doctrinal method in legal scholarship. *Oxford Journal of Legal Studies, 40*(2), 303–328.

Ministry of Information Technology and Telecommunication. (2025). *National Artificial Intelligence Policy*. Government of Pakistan. https://moitt.gov.pk/SiteImage/Misc/files/National%20AI%20Policy.pdf

National Institute of Standards and Technology. (2023). *AI risk management framework (AI RMF 1.0)*. U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework

Sahar, G. (2026). An analysis of international best practices for the ethical use of AI in justice sector and formulation of guidelines for use of generative AI by judiciary in Pakistan (Working Paper). SSRN. https://doi.org/10.2139/ssrn.6573258

Said, G., Azamat, K., Ravshan, S., & Bokhadir, A. (2023). Adapting legal systems to the development of artificial intelligence: solving the global problem of AI in judicial processes. *International Journal of Cyber Law*, *1*(4).

Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review*, *35*(4), 1305–1334. https://readingroom.law.gsu.edu/gsulr/vol35/iss4/10/

Seng, D., & Mason, S. (2021). Artificial intelligence and evidence. *Singapore Academy of Law Journal*, *33*, 241–279. https://search.informit.org/doi/10.3316/informit.856086196428655

Stoykova, R. A. (2024). A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review*, *55*, 106040.

Stoykova, R., Bonnici, J. M., & Franke, K. (2023). Machine learning for evidence in criminal proceedings: Techno-legal challenges for reliability assurance. *AI in forensic sciences*, 21.

Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, *41*, 105567.

White, P. J. (2024, July 20). *AI and evidence: What should judges look for?* Paper presented at the 2024 Forum for State Appellate Court Judges, Nashville, TN.

Zarsky, T. (2016) The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology, & Human Values*, *41*(1), 118–132. https://doi.org/10.1177/0162243915605575