



Journal of Multidisciplinary and Translational Research (JMTR)

journal homepage: <https://journals.kln.ac.lk/jmtr/>



Admissibility of AI-generated digital evidence in criminal proceedings: A framework for enhancing judicial reliability in Sri Lanka

M.N.D. Jayasumana^{1*}

¹IDM Nations Campus International, Colombo 06, Sri Lanka

Abstract

Generative AI, synthetic media, facial recognition, and a range of other evidence tools and analytics powered by machine learning (hereinafter referred to together as “ML tools and analytics”) have transformed the evidence landscape in criminal proceedings. Traditional evidence such as emails and other electronic documents and records, as well as physical evidence such as photographs and videos of scenes of crime and extracts of data from mobile phones, are now frequently joined by a wide variety of new evidence generated by, modified with, or analyzed by ML tools and analytics (hereinafter referred to together as “AI evidence”). This article undertakes a doctrinal and comparative legal analysis, supplemented by a forensic-governance assessment of the legal, procedural and auditable controls governing the generation, preservation, processing, disclosure and courtroom use of AI-mediated evidence, with particular reference to Sri Lanka. The framework of rules provided by the Evidence (Special Provisions) Act No. 14 of 1995; the Electronic Transactions Act No. 19 of 2006 as amended; the Code of Criminal Procedure Act No. 15 of 1979; the Computer Crime Act No. 24 of 2007 and the case law on the various requirements of proof with respect to evidence, such as proof of authenticity; safe custody; disclosure; and fairness, that currently apply to evidence adduced in criminal trials in Sri Lanka are identified and analyzed. The article also highlights the lacunae in the admissibility framework of evidence currently in place by providing an analysis of the rules on admissibility of evidence in England and Wales, in the European Union and in a number of recent Indian cases on synthetic evidence with particular reference to issues that arise in relation to the admissibility of expert evidence; safe custody of such evidence; fairness; the rules of evidence; proportionality; digital disclosure; and the auditability of evidence. Finally, the article proposes a hybrid framework of rules on admissibility that is derived from the existing rules on admissibility of evidence and a range of instruments that govern the use of evidence in legal proceedings including forensic science regulation; evidence handling standards; AI-governance instruments; and model documentation practices. Such a framework of rules on admissibility of evidence is proposed to be tailored to the conditions in Sri Lanka and would consist of an AI-Evidence Certificate; provenance requirements; audit trail requirements; the duties of disclosure by parties adducing such evidence; and verification of such evidence by an independent expert where necessary, in addition to a judicial review checklist of concerns specific to such evidence. In summary, what Sri Lanka requires are a limited number of amendments and practice notes that translate the rules on admissibility of evidence currently in place into the AI-era of machine-generated evidence while maintaining the fundamental principles of fairness.

Keywords: AI-generated evidence, Criminal proceedings, Digital evidence, Judicial reliability, Sri Lanka

Article info

Article history:

Received 30th April 2026

Received in revised form 10th June 2026

Accepted 15th July 2026

Available online 25th July 2026

ISSN (E-Copy): ISSN 3051-5262

ISSN (Hard copy): ISSN 3051-5602

Doi:

ORCID iD: <https://orcid.org/0009-0006-6168-0929>

*Corresponding author:

E-mail address: danu.jayasumana@yahoo.com

(M.N.D. Jayasumana)

[CC BY-NC-SA](#) © 2026, The Author(s)

Introduction

For the purposes of this article, “digital evidence” includes electronic records and data obtained from computers, mobile devices, networks, audio-visual systems, and cloud platforms, together with associated source files, metadata, logs, and evidential outputs generated, modified, enhanced, classified, or analysed using artificial intelligence (AI) systems. In the criminal courts of Colombo, video evidence is increasingly adduced in criminal proceedings, presenting trial judges with questions of admissibility that existing evidentiary law was not specifically designed to address. Consider, for example, a prosecution that seeks to tender a video recording that clearly depicts the accused at the scene of the alleged offence. The defence objects on the basis that the recording may have been generated by AI or materially altered or enhanced using AI technologies. At present, there is no clearly established procedure requiring the production of relevant AI-system documentation, including, where applicable, a model card, nor is there a specific statutory requirement compelling an investigating officer to produce cryptographic hash records relating to the original digital capture. The trial judge may therefore be left without a structured judicial checklist or recognised methodology for determining whether the recording is authentic, wholly AI-generated, or materially AI-enhanced in a manner that cannot be independently verified by a witness, including the officer through whom the evidence is produced. More broadly, the existing law of evidence in Sri Lanka does not provide a comprehensive procedural framework specifically designed to address the authenticity, provenance, integrity, transparency, and verification challenges presented by AI-generated and AI-mediated digital evidence. The critical questions are therefore these: by what process was the evidence generated, acquired, or transformed; who exercised control over that process; can its authenticity, provenance, and integrity be independently verified; and is it fair to rely upon such evidence in determining the guilt or innocence of an accused person?

This article makes four principal contributions. First, it critically evaluates the existing Sri Lankan legal framework governing electronic and computer-generated evidence and identifies its limitations when applied to AI-generated and AI-mediated evidence. Second, it undertakes a comparative analysis of relevant legal and regulatory approaches in England and Wales, the European Union, and India in order to identify principles capable of informing reform in Sri Lanka. Third, it integrates principles derived from digital forensics, forensic governance, and IT auditing into the legal analysis of authenticity, provenance, integrity, disclosure, and verification. Fourth, drawing upon these doctrinal, comparative, and multidisciplinary insights, it proposes a hybrid framework for Sri Lanka comprising an AI Evidence Certificate, provenance and disclosure requirements, independent verification where necessary, and a structured judicial checklist for assessing the admissibility and reliability of AI-generated and AI-mediated digital evidence.

Practice often will encounter various forms of digital evidence that were produced by AI, or assisted by AI, in four different scenarios: (1) Fabricated evidence: deepfakes which are so realistic that they could be used to incriminate a person by falsely portraying him or her at a scene of a crime or in a conversation with another person; (2) Evidence facilitated by AI: digital evidence which has been produced with the assistance of AI in order to exculpate a person or to provide other evidence; (3) Machine-assisted investigative procedures: various machine-assisted procedures that investigators use when conducting an investigation, including, for example, face comparison, image and video enhancement, clustering, automatic transcription of audio recordings, and identification of people in images and videos using data that already is available;

(4) AI-generated metadata: metadata generated by AI systems, the information contained in such metadata assist in authenticating the digital evidence in question by providing information on the provenance of the digital evidence in question.

In contrast, the vast majority of recent publications dealing with AI evidence from England and Wales, the European Union and India focus on the issue of transparency, that is, the potential for bias, explainability of a computer program or AI system and the risk of deception on the part of such a system where its output could have serious consequences and be used as evidence in legal proceedings. In contrast, the applicable case law in Sri Lanka is some twenty odd years old dealing with the issue of tampering with computer generated evidence. Thus, while the Evidence (Special Provisions) Act 1995 enables recorded or computer generated evidence to be adduced in a court of law subject to certain conditions and the Electronic Transactions Act 2006 sets out to establish the legal evidence of information communicated in electronic form, both pieces of legislation pre-date the development of modern generative AI and therefore do not expressly address several AI-specific concerns, including provenance, model versioning, transformation histories, or the validation of machine-generated outputs. This does not necessarily make the existing framework inapplicable; rather, it raises the question whether general electronic-evidence principles can be interpreted to accommodate AI-mediated material and where additional procedural safeguards are required. Instead, however, the rapidly developing synthetic media technologies can and do in fact generate vast amounts of such evidence many of which would not be readily recognizable as such.

A large body of literature currently exists addressing issues that surface in relation to the use of AI generated evidence, whether it be in relation to electronic evidence, digital forensics, the explainability of AI, or the governance of trustworthy AI. In addition to the aforementioned, there is an ever-increasing body of judicial and policy authority emerging on issues in relation to the use of deepfakes, algorithmically generated facial recognition images, and other evidence that may be extracted from a variety of different devices. Importantly, however, there is currently a paucity of literature addressing an integrated approach to the management of such evidence in criminal proceedings and drawing upon appropriate jurisprudence, as well as materials from criminal procedure in other jurisdictions, as well as from a variety of the various different forensic sciences that are typically adduced in criminal proceedings. The wider literature on AI governance, measurement, and risk is generally concerned with the measures needed to govern AI systems responsibly, to measure their impact, and to manage the risks arising from their use. Explainability recurs across these measures as a central requirement. In its work on explainability of AI systems, the *NIST (Phillips et al., 2021)* notes that, for an AI system to provide evidence in support of a conclusion or assertion, that system must explain the evidence that it relied upon. Importantly, such an explanation must be meaningful; it must be faithful to the actual processes that the model has undertaken; and it must also acknowledge any limitations on the part of that model that are to be relevant to the matter at hand.

Methodology

This article uses a qualitative doctrinal and functional comparative legal methodology. The doctrinal part examines primary legal materials such as legislation, judicial decisions, and procedural rules. These materials relate to electronic records, criminal disclosure, computer-crime investigations, and the admissibility of evidence. The study also considers relevant

secondary literature and forensic-governance standards. It addresses three main research questions. First, to what extent can the existing Sri Lankan legal framework deal with AI-generated and AI-mediated digital evidence? Second, what limits arise when that framework is applied to issues such as authenticity, provenance, integrity, transparency, disclosure, and fairness? Third, what legal, procedural, and forensic-governance measures can be drawn from Sri Lankan law and selected foreign jurisdictions to develop a suitable framework for Sri Lanka? A doctrinal approach is appropriate because the study focuses on interpreting and evaluating legal rules and procedures. It does not seek to measure behaviour or test the technical performance of specific AI systems.

The comparative part follows a functional approach. It examines England and Wales, the European Union, and India as reference jurisdictions. These jurisdictions were selected because they offer different but complementary approaches to digital and AI-related evidence. England and Wales has a developed system of criminal procedure, expert-evidence rules, and forensic-science regulation. The European Union provides a rights-based framework dealing with artificial intelligence, data protection, transparency, and law-enforcement processing. India offers a comparable common-law setting and has significant judicial experience with electronic evidence, certification, digital authenticity, and emerging disputes involving synthetic media. The comparison is not intended to be exhaustive. Its purpose is to identify useful principles and safeguards that may be adapted to the Sri Lankan context.

The article also examines the evidentiary lifecycle as a forensic-governance framework. It considers whether the main stages of that lifecycle are subject to proper and auditable controls. These stages are: (i) capture, (ii) preservation, (iii) transfer, (iv) storage, (v) processing, (vi) transformation, (vii) disclosure, (viii) expert review, and (ix) courtroom presentation. Particular attention is given to preservation, chain of custody, provenance, audit trails, validation, disclosure, and independent verification.

The key question is not simply whether an AI system can produce accurate results in general. The more important issue is whether there is enough assurance about how the particular evidence was generated, preserved, processed, and disclosed in the case before the court. This helps the court decide whether the evidence should be admitted, admitted with safeguards, given less weight, or excluded.

The study is entirely qualitative and non-empirical. It does not involve surveys, interviews, fieldwork, experiments with AI tools, statistical analysis, or data collected from human participants. It relies on publicly available legal, regulatory, technical, and scholarly materials. The criteria developed in the article are rights-oriented. They are intended to ensure that AI-mediated evidence is used in a lawful, reliable, and fair manner. Disclosure should therefore be proportionate to the evidentiary purpose for which the material is relied upon. It should also avoid unnecessary interference with privacy and other protected interests. The proposed framework seeks to balance effective scrutiny of AI-mediated evidence with appropriate judicial control. This approach is consistent with fair-trial principles, including the Sri Lankan Supreme Court's interpretation of section 162 of the Code of Criminal Procedure Act in relation to prosecutorial disclosure and the use of digital material in criminal proceedings.

Results

Sri Lanka already has a more developed legislative and judicial framework of evidence for electronic information than is acknowledged by many. What is needed is a strengthening of the four main statutes and the cases that have addressed them in order to meet the new demands of the AI era.

The other evidence namely recorded and computer-generated evidence were dealt with by the legislature when the Evidence (Special Provisions) Act No. 14 of 1995 was enacted. This Act was introduced to supplement the Evidence Ordinance currently in force. The categories of evidence specified in the Evidence Ordinance such as documents, statements, real evidence, etc. were not found to be sufficient to deal with the various types of recorded and computer-generated evidence generated and used today. Therefore, the said Act made specific provisions in respect of recorded evidence by setting out four special circumstances in which such evidence would be admitted as evidence. Such circumstances are (i) contemporaneous recording of the facts, (ii) safe custody of the record, (iii) precautions taken to prevent tampering of the record and (iv) other circumstances. The courts in Sri Lanka have consistently interpreted the said four circumstances in a manner that compliance with such circumstances would be sufficient for the admission of evidence and would be considered as substantive rather than procedural requirements. In the case of *Abeyagunawardane v. Samoon and Others* the Court of Appeal laid down the conditions to be satisfied for the admissibility of secondary evidence of a document. According to the said decision sufficient evidence must be adduced to show that the primary evidence had been (i) contemporaneously recorded, (ii) kept in safe custody and (iii) sufficient precautions had been taken to prevent any alteration to the record. Such decision is still relevant today not because it deals with AI generated evidence but because the principles of law laid down in that case would apply to any evidence generated through computers and would be relevant to the issue of the reliability of such evidence.

The Electronic Transactions Act No. 19 of 2006 (as amended by Act No. 25 of 2017) gives legal recognition to communications and records generated and sent by means of information and communication technology, including electronic records and data messages, and provides rules relevant to electronic signatures and the legal effect of electronic communications. Although the Act was enacted before modern generative AI, its general provisions are not necessarily incapable of applying to AI-mediated digital material where the statutory requirements are otherwise satisfied. The difficulty is that the Act does not expressly address AI-specific questions such as the provenance of a generated output, the model and version used, the history of material transformations, or the validation and limitations of the system. Accordingly, the existing statutory framework may provide part of the legal foundation, but additional evidentiary proof may be required to establish that an AI-generated or AI-mediated record is sufficiently authentic, reliable, and traceable for the purpose for which it is tendered.

The admissibility and disclosure of evidence in criminal proceedings are governed by the applicable law of evidence and criminal procedure. In the significant Supreme Court decision of *De Vas Gunawardane and Others v. Attorney General*, arising from proceedings before a High Court at Bar, the Court considered the prosecution's failure to comply with section 162 of the Code of Criminal Procedure Act, as amended. The Supreme Court held that section 162 reflects the principle of a fair trial and imposes a mandatory duty on the prosecution to provide a list of the

witnesses and productions it intends to rely upon, together with the material falling within section 162(2) of the Code. The Court further emphasized that the prosecution's disclosure obligation extends to the material it intends to use at trial. Applied to AI-mediated evidence, where the prosecution intends to rely on an AI-enhanced facial comparison, meaningful disclosure should therefore include the source image, the relevant transformation or processing logs, the AI model and version used, and any material information concerning the system's methodology, confidence measures and limitations that is necessary to permit the reliability of the resulting evidence to be assessed.

The Computer Crime Act No. 24 of 2007 is also relevant to the present analysis, although it was enacted primarily to address forms of computer misuse rather than the admissibility of digital evidence. Where the creation, alteration, modification or deletion of digital material through the use of AI involves conduct falling within an offence created by the Act, the relevant conduct may attract criminal liability if the statutory elements are established. The significance of the Act for the present analysis lies principally in its recognition of computer-related investigations, digitally stored material and the importance of appropriate technical expertise in investigating and establishing technologically mediated facts. Accordingly, where the reliability of AI-generated or AI-mediated evidence depends upon technical matters that cannot adequately be established through ordinary observation, independent expert verification may be necessary.

Sri Lankan courts have historically approached computer-generated evidence with particular attention to authenticity, safe custody and the risk of alteration or tampering. Decisions such as *Abu Bakr v. The Queen*, *Benwell v. Republic of Sri Lanka* and *Abeyagunawardane v. Samoon and Others* illustrate the continuing importance of establishing the integrity of technologically generated evidence before reliance is placed upon it.

Practice within England and Wales takes a significantly more developed approach to the required procedural content. Section 78 of the Police and Criminal Evidence Act 1984 enables a court to exclude evidence adduced by the prosecution on the grounds that it would be unfair to admit the same. Accordingly, evidence generated by a computer which has been produced in opaque circumstances would be excluded if there has been no independent testing of the same to verify its reliability. Moreover, that which is required to be disclosed by an expert witness in accordance with Part 19 of the Criminal Procedure Rules (as amended from time to time) would extend to that which has been generated by a computer system. In order to rely on such evidence, the following information would need to be disclosed: (i) the qualifications of the expert; (ii) the material upon which the expert has relied; (iii) the methods employed by the expert; (iv) the instructions received by the expert from any person. An expert has an overriding duty to assist the court. In giving expert evidence, an expert shall only express an opinion on a matter on which they are qualified to give such evidence and shall not suggest any course of action and, accordingly, the required disclosure in relation to AI generated evidence shall be concerned with two issues, namely the reliability of technical evidence and the unfairness of one-sided use of a model.

In terms of the wider forensic governance environment in Sri Lanka, there is currently none in place regarding the admissibility of evidence however there are provisions in place in England and Wales regarding the admissibility of evidence that could be useful for comparisons. The statutory code of practice of the Forensic Science Regulator for activities undertaken in relation

to criminal investigation and the criminal justice system sets out minimum quality standards for all forensic activities. This includes provisions such as the following: (i) the continuous retention of all exhibits, whether physical or computer based, from the time of their collection until they are disposed of; (ii) the unique identification of all items of evidence at all times; (iii) the use of valid and relevant methodology in arriving at any conclusions in relation to any evidence; and (iv) the maintenance of and reference to detailed documentation in relation to all stages of the forensic process. Provisions exist in relation to the extraction of data from a device such as that set out by the Home Office (2023) and the requirements that must be observed by any person authorized to extract device containing data and work with such device. There are also four broad criteria that must be considered in relation to the inspection of any digital evidence in order to ensure that any such inspection is fair. These are that the inspection is: (i) justified; (ii) proportionate to the alleged offence and (iii) carried out in such a way as to avoid any element of oppression. The principles of *Bater-James* ([2020] EWCA Crim 790) provide useful criteria for consideration in this regard.

Although *Bridges v. Chief Constable of South Wales Police* did not arise in the context of criminal proceedings, the decision is relevant to the present analysis because it illustrates that outputs produced through algorithmic systems should not be treated as inherently neutral. It highlights the need for an affirmative assessment of matters such as bias, lawfulness and the potential impact of the technology concerned. Accordingly, where a party seeks to rely on AI-generated or AI-mediated evidence, that party should establish that the system or model used was appropriate for the particular evidentiary purpose, had been adequately tested and validated, and that any material limitations or risks of bias had been identified and disclosed.

More broadly, AI-generated evidence may also be considered within a distinct technical and evidentiary framework, supported by a growing body of standards and governance instruments. For example, NIST's AI RMF 1.0 provides a framework for governing AI systems throughout their lifecycle, including their design, development, deployment and use, with particular emphasis on the identification and management of risk. *Phillips et al. (2021)* identifies four principles of explainability: (i) evidence, referring to the basis of the AI system's output; (ii) meaning, requiring the output to be intelligible to its users; (iii) correctness, requiring the explanation to accurately reflect the process performed by the AI system; and (iv) knowledge limits, requiring the system to recognize circumstances in which it operates beyond its validated scope.

The model-card literature (Mitchell et al., 2019) similarly emphasizes the importance of documenting the intended uses of high-impact models, together with information concerning their performance, limitations and relevant ethical considerations. In digital forensics, evidence of activity on a computer or network is acquired, preserved, analysed and presented in accordance with technical standards, including NIST SP 800-86 (Kent et al., 2006) and SWGDE guidance (Scientific Working Group on Digital Evidence, 2024, 2025). These standards emphasize, inter alia, (i) the secure acquisition of digital evidence; (ii) the preservation of evidence in its original state; (iii) contemporaneous documentation of the steps undertaken during analysis; and (iv) maintenance of an appropriate chain-of-custody record.

Technical standards have also been developed to support verifiable claims concerning digital assets, including C2PA Content Credentials (Coalition for Content Provenance and Authenticity, 2026). Such mechanisms enable the creation and use of verifiable credentials associated with

digital assets, comprising claims relating to an asset, assertions supporting those claims, and cryptographic signatures attributable to the entities responsible for creating or managing those claims and assertions.

National Stock Exchange of India Ltd. v. Meta Platforms Inc., Interim Application (L) No. 21456 of 2024 in Commercial IPR Suit (L) No. 21111 of 2024 (Bombay High Court 2024), was a commercial suit for trademark infringement and passing off brought by the National Stock Exchange of India Limited against Meta Platforms Inc. and others, in which the Court granted urgent interim relief directing the takedown of deepfake videos falsely showing the Exchange's Managing Director endorsing stock-picking services on Meta's social media platforms. A comparable urgency is evident in *Akshay Hari Om Bhatia v. John Doe*, where the Bombay High Court granted ex parte interim relief restraining the unauthorised use of an actor's name, image, voice and likeness in AI-generated deepfake content, recognising an enforceable personality right that could be protected in the wider public interest independently of any criminal proceeding. *Hameed v. State by Bidadi Police, Criminal Petition No. 10135 of 2025* on the other hand, was a case where the CCTV footage in question was secondary evidence and no satisfactory material or satisfactory evidence was adduced to prove that the said footage was not capable of being tampered with. The court held that in such circumstances section 65B of the Evidence Act, 1872 would apply. In other words, the said case treated the possibility of manipulation of evidence by way of AI as a relevant issue that requires to be proven with due evidence and to be certified under section 65B of the Evidence Act, 1872. In fact, as observed above, the said case would also lead to the conclusion that where any evidence is transformed by AI, it would be necessary for the party adducing such evidence to disclose the same and to further prove the correctness of such evidence by means of independent evidence. The doctrinal and comparative findings can be summarized across jurisdictions as follows (Table 1). These comparisons are grounded in official statutes, judgments, and guidance.

Table 1: Comparative legal position on AI-generated digital evidence (*continued on next page*)

Jurisdiction	Core legal instruments	Leading authorities and guidance	Dominant admissibility concern	Practical lesson for Sri Lanka
Sri Lanka	Evidence (Special Provisions) Act 1995; Electronic Transactions Act 2006; Code of Criminal Procedure Act 1979; Computer Crime Act 2007	Abeyagunawardane v. Samoon; Q. v. <i>Abu Bakr v. The Queen</i> and Benwell; Supreme Court fair-trial disclosure jurisprudence under section 162	Authenticity, safe custody, anti-tampering safeguards, fair-trial disclosure	Existing law is usable but AI-specific provenance, logging, and explainability requirements are absent
England and Wales	PACE 1984 s.78; Criminal Procedure Rules Part 19; Forensic Science Regulator Code (2025); Home Office	<i>Bridges</i> ; <i>Bater-James</i> principles; expert evidence guidance; Forensic Science Regulator Code (2025)	Fairness, expert neutrality, proportionality, continuity, method validity, bias inquiry	AI-mediated proof should be screened through expert disclosure, quality standards, and fairness discretion

Jurisdiction	Core legal instruments	Leading authorities and guidance	Dominant admissibility concern	Practical lesson for Sri Lanka
	device-extraction code			
European Union	AI Act; Law Enforcement Directive; e-evidence framework	European Commission guidance on Article 50 and transparency code of practice	Transparency, law-enforcement data safeguards, anti-deception, labelling of synthetic content	Provenance and disclosure should be treated as part of legality and reliability
India	Electronic-evidence procedure; court rules on hash-based filing; IT Rules and deepfake response	<i>Akshay Tanna; Anil Kapoor; Chaitanya Rohilla; NSE v. Meta; Akshay Hari Om Bhatia; Hameed</i>	Deepfakes, hash integrity, section 65B compliance, intermediary response, public deception	Courts are already linking synthetic-media risk with authenticity, certification, and urgent protective orders

Discussion

The proposed hybrid approach responds to a basic feature of the problem: AI-generated evidence cannot be admitted or excluded on a simple ‘admit’/‘deny’ basis, because no single threshold could fairly capture the range of ways in which such evidence is produced. What is important is whether the party adducing the evidence has established sufficient process assurance that the court can be satisfied that the evidence is relevant and, more importantly, authentic (as opposed to merely reliable or plausible) and has not been tampered with (except disclosure made). The same can be achieved from a legal perspective by requiring that the generated AI-evidence is authenticated, disclosed and a fair trial is held. The comparative analysis of approaches identified for the admissibility of generated AI-evidence by the professional communities involved found that they were not in conflict with each other but were different articulations of the same demand.

The hybrid framework rests on four linked components: an AI Evidence Certificate completed by the party producing the evidence; a judicial admissibility checklist applied by the court; staged legislative and practice-direction reform; and institutional and training measures for the police, prosecutors and the judiciary. They are set out below in the order in which they build upon one another, rather than the order in which they would typically arise in a given case.

The AI Evidence Certificate: The Producer Must Prove a Case. To tender AI-generated evidence or evidence which has been materially transformed by AI, whether as prosecution evidence, as defense evidence or as expert evidence introduced by a third party, a party must produce an AI Evidence Certificate. The Certificate must be completed by the person responsible for the production of the evidence, by the person who conducted an investigation which the evidence relied upon, by the expert who produced the evidence, and by the producing authority. There must be annexures to the Certificate. The minimum information that must be provided in the body of the Certificate is: The source exhibit identifier; The date and time that the source exhibit

was acquired; Hash values for the source exhibit and for the evidence subsequently produced; Where the evidence subsequently produced is a file then the storage location and the access record for that file; A description of all processing that has been applied to the source exhibit to produce the evidence subsequently produced; Whether the entire of the evidence subsequently produced was generated by AI; Whether any part of the evidence subsequently produced was enhanced by AI; Whether any part of the evidence subsequently produced was analyzed by AI; The name of the tool or model; The provider of the tool or model; The version number of the tool or model; Any settings or any prompts that were used for any processing that was applied to the source exhibit; A record of every intervention by a human made to any processing that was applied to the source exhibit at any stage; The confidence scores produced by the system or the error rates produced by the system; The known limitations of the model when used for the analysis of the content of the source exhibits for the purposes for which the evidence subsequently produced is tendered; Whether the evidence subsequently produced is C2PA content credentials or whether the evidence subsequently produced is equivalent cryptographic provenance signatures. Where the AI system is an enterprise system then a model card and a system card and a validation study and vendor assurance documents etc would be annexures to the Certificate. Of course, the Certificate of a vendor-supplied system would also include a model card and a system card and a validation study and vendor assurance documents etc. The purpose of requiring a producer to complete a certificate is the same as the purpose of requiring a person to complete a chain of custody record for evidence and the same as the purpose of requiring an expert to complete an expert disclosure for technical evidence, i.e. so that the court is able to determine the reliability of the produced evidence. If a party is unable to complete a certificate because the generating system does not provide an audit trail then that inability to complete a certificate is further evidence, i.e. it is further evidence of the unreliability of the evidence subsequently produced by the generating system and the court must draw the necessary inferences in regard to the weight to be given to the produced evidence or in regard to the admissibility of the produced evidence.

The Judicial Admissibility Checklist: Nine Questions for the Court.

- | | |
|---------------------------------------|--|
| 1. Legality | : Was the source data lawfully obtained, processed, and retained? |
| 2. Relevance | : Does the output prove, disprove, or materially assist a fact in issue? |
| 3. Authenticity | : Can the producing party prove source, authorship, and transformation history? |
| 4. Integrity | : Are source and output files hashed, logged, and preserved with an unbroken custody record? |
| 5. Transparency | : Has the party disclosed enough about the tool, version, method, and intervention to permit challenge? |
| 6. Validity | : Is the process supported by expert evidence, validation material, or recognized standards? |
| 7. Bias and limitation | : Are there known risks of demographic bias, hallucination, confidence inflation, or out-of-scope use? |
| 8. Fairness | : Would admission without further disclosure, verification, or limiting directions cause unfair prejudice? |
| 9. Weight versus admissibility | : If concerns are partial rather than fatal, should the court admit the evidence with caution rather than exclude it entirely? |

This checklist is not a substitute for discretion. It is a discipline for discretion. It channels the underlying logic already visible in section 78 PACE, Sri Lankan fair-trial disclosure jurisprudence, and the bias inquiry in *Bridges*.

A practical courtroom workflow is given in Figure 1.

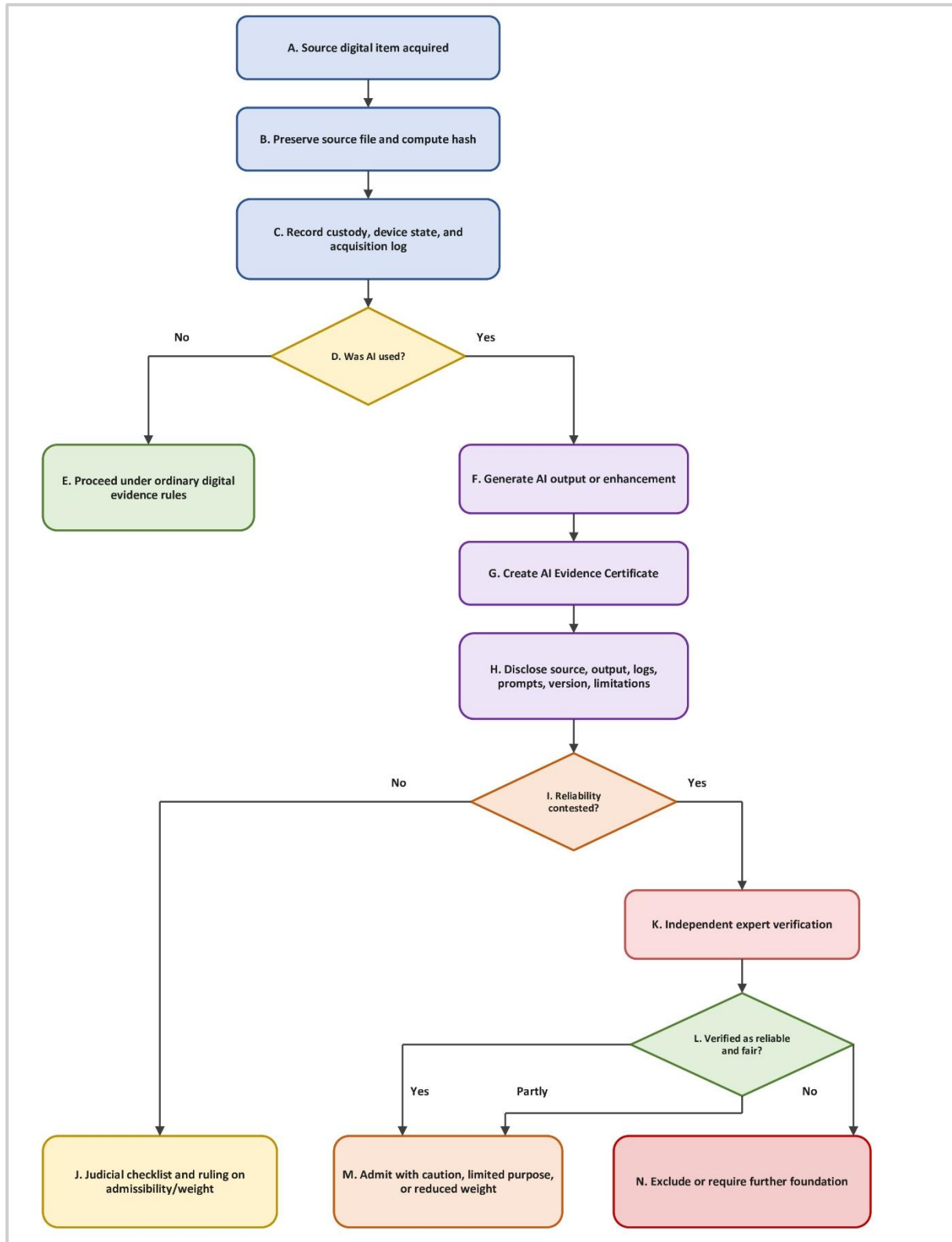


Figure 1. Proposed workflow for assessing AI-generated digital evidence in criminal proceedings

Legislative and Practice-Direction Reform: Four Staged Steps.

1. In the short term, there is the possibility of immediate practice being solidified by legislative amendment in due course. In the first instance, a joint practice direction should be issued by the judiciary, the Attorney General's Office and the police digital-forensics units. Such a practice direction would serve to clarify what is meant by the term 'evidence generated by means of artificial intelligence' for criminal justice purposes. In addition, it would set out the minimum information required to be provided in relation to AI generated evidence for an AI Evidence Certificate to be issued. Furthermore, the practice direction should require the preservation of hashing and processing logs for all AI generated exhibits. Finally, it would require the disclosure of that which is generative, enhancing or analytical in relation to processing where material to assessing the evidence's reliability.
2. Reform the Evidence (Special Provisions) Act by introducing provisions that specifically address synthetic evidence, such as (i) evidence generated by means of AI that are recordings (whether audio or video) and/or documents and by proving the circumstances of the recording and providing safe custody of the said recording as well as a record of the said recording's transformation history and the measures taken to prevent any unrecorded changes to the said recording and/or its constituent parts, as well as safe custody of any source artefacts; and
3. Reform section 162 of the Code of Criminal Procedure Act to specifically require the disclosure by the prosecution of material metadata, processing logs and information regarding the reliability of any AI-exhibits of evidence adduced by the said prosecution in any criminal proceedings; and
4. Reform the Electronic Transactions Act to specifically provide that the presumptions in section 4(1) of the Act regarding records generated by means of information and communication technology would not abrogate the fundamental requirements of proof for any and all AI-generated evidence (including but not limited to evidence that has been altered in some material respects by AI).

Institutional Reform & Legislation: In the first place, the police and the forensic units must keep a record of the processing tools' versions that have been used for the evidence collection; of all processing activities' records with sufficient logging to be able to establish a chronological order of events; keep all the evidence in a secure storage with the necessary means to prevent any tampering with the evidence and to maintain adequate and immutable audit trails (similar to the transaction logs that financial institutions keep). Moreover, when the police utilize vendor-supplied AI processing tools for the purposes of the criminal investigations, similar scrutiny must be applied to their procurement as to any other product or service; i.e. due diligence, validation, ability to provide explainability of the decisions made by the system, ability to export the processing activities' logs, support for the evidence's cryptographic provenance, transparency regarding the processing intended for and the limitations of the system. Lastly, all legal professionals (judges and prosecutors) need specific training, not a general introduction to how AI functions but rather specific training regarding deepfakes, voice cloning, facial recognition, image and other evidence enhancement, confidence scores in decision-making and most importantly the crucial distinction between a system's claimed accuracy and the system's error

rate as measured and for a specific population or in a specific context. In summary, the justice system must transition from a position of blind trust of black-box AI to a position of control-based assurance where the extent to which one can trust the output of a process is equal to the degree to which one can verify the process that generated the output in the first place.

A model implementation matrix for Sri Lanka is set out in Table 2. The components are designed to work together. A certificate without disclosure is incomplete; disclosure without expert verification may be insufficient where the technical issues are genuinely complex; and both are diminished without a judicial checklist that brings them to bear at the point of decision.

Table 2: Proposed implementation matrix for Sri Lanka

Reform component	Minimum operational content	Recommended legal vehicle
AI Evidence Certificate	Hashes, provenance, model/tool name and version, prompts/settings where material, processing logs, human interventions, limitations, validations, sign-off	Practice direction immediately; statutory schedule on amendment of Evidence (Special Provisions) Act
Disclosure rule	Source files, output files, metadata, processing logs, error/bias materials, prior inconsistent outputs, vendor or laboratory documentation where relied upon	Amendment to Code of Criminal Procedure Act, section 162; prosecutorial circular
Expert verification	Reproducibility test, artefact examination, bias/limitation analysis, methodology note, version-specific performance review	Criminal Procedure Rule or supplement to Evidence Ordinance
Provenance control	Chain of custody, immutable audit trail, access logging, secure evidence repository, retention schedule, C2PA or equivalent credentials where available	Police and forensic SOPs; ministerial regulations
Judicial screening	Reliability checklist, power to order further foundation evidence, limited-purpose admission, or exclusion with reasons	Judicial practice direction and bench guide
Accreditation and training	Technical competence standards, courtroom testimony preparation, tool validation, continuing judicial education	Administrative policy; Judicial Service Commission and Bar Association programmes

Three limitations of the framework deserve acknowledgment, partly because honesty about limits strengthens rather than undermines the proposal. Commercial and proprietary AI systems frequently cannot or will not disclose training data, architecture, or internal logic. An absolute explainability threshold, requiring full transparency as a condition of admissibility would exclude large classes of commercially developed forensic tools and may not be technically achievable even with willing vendors. The better standard is practical sufficiency: is enough information available

to permit a fair evaluation of reliability for this specific use in this specific case? That is a contextual judgment, and it should remain one.

Provenance tools such as C2PA content credentials are genuinely valuable, but their value is conditional. The presence of a valid content credential strengthens authenticity; its absence does not prove fabrication; and its presence does not cure every methodological or bias-related defect in the underlying AI process. Courts should treat provenance metadata as one element in a multi-factor reliability assessment, not as a determinative certification.

Finally, not every AI interaction is legally material. Format conversion, lossless compression, or routine metadata extraction does not engage the same reliability concerns as generative reconstruction, face comparison, or synthetic voice generation. The framework is calibrated to reflect this: the more significant the AI's role in transforming or creating evidentiary content, and the less transparent the process, the greater the legal scrutiny warranted. Proportionality is built into the design.

Open questions and limitations: This study is doctrinal and comparative rather than empirical. It does not test any specific AI tool in the Sri Lankan forensic environment, and some Sri Lankan case law on electronic evidence remains thinly reported or difficult to access in official repositories. The recommendations should therefore be read as a high-confidence legal-policy framework that would benefit from future empirical validation through judicial, prosecutorial, and forensic practice studies.

Conclusions

There is a temptation, when confronting a technology as powerful and as rapidly evolving as generative AI, to call for comprehensive new legislation. That call should be resisted; not because the challenge is minor, but because Sri Lanka's existing legal resources are more capable than they are often given credit for, and because comprehensive legislation enacted without practice experience tends to produce either over-inclusive rules that exclude reliable evidence or under-inclusive rules that admit unreliable exhibits. The better approach, and the one this article defends, is targeted procedural reform anchored in existing legal principles.

Sri Lanka's courts have consistently held that technological sophistication does not substitute for demonstrable integrity. That holding predates AI. It does not need to be legislated again; it needs to be operationalized for the AI environment given procedural teeth through a certificate requirement, a disclosure obligation, expert verification standards, and a judicial checklist. Each of those elements is either already present in embryonic form in Sri Lankan law or is directly supported by principles that Sri Lankan courts already accept.

The comparative experience of England and Wales, the European Union, and India converges on the same conclusion from different institutional directions. Reliable AI-era adjudication requires procedural discipline: provenance documentation, validated methodology, bias scrutiny, calibrated disclosure, and structured judicial control. These are not foreign imports. They are the evidentiary requirements of a system that takes seriously both the probative value of technical evidence and the irreversible consequences of convicting on unreliable material.

The practical path forward is staged. A joint practice direction can be issued now, clarifying disclosure requirements and prescribing the minimum contents of an AI Evidence Certificate. Statutory amendments to the Evidence (Special Provisions) Act, the Code of Criminal Procedure Act, and the Electronic Transactions Act can follow as experience accumulates. Training programs for judges, prosecutors, and defense practitioners can be developed in parallel. None of this requires Sri Lanka to wait for a regional or international consensus; the legal resources and institutional capacity to begin are already available.

Ultimately, what the AI era demands of criminal evidence law is not a new philosophy but a renewed commitment to an old one: that the weight placed on a piece of evidence in a criminal trial should be proportionate to the verifiability of the process that produced it. In a justice system increasingly confronted by synthetic media and automated analytics, judicial reliability will depend less on the persuasiveness of an exhibit's appearance and more on the auditability of its origins.

Acknowledgements

The author gratefully acknowledges the constructive comments and guidance provided by the editorial reviewers and the Editorial Office of the Journal of Multidisciplinary and Translational Research (JMTR). Their observations contributed to improving the clarity, structure, and presentation of this article.

Declaration of Funding Sources

No external funding was received for this study.

Conflict of interest statement

The author declares no conflict of interest.

Data availability statement

No new datasets were generated or analysed in this study. The article relies on publicly available legal, regulatory, technical, and scholarly materials.

Author Contribution

Sole author; responsible for conceptualization, legal analysis, comparative synthesis, framework design, drafting, and revision.

References

- Abeyagunawardane v. Samoon*, [2007] 1 Sri L.R. 276. <https://www.lawnet.gov.lk/wp-content/uploads/2016/11/030-SLLR-SLLR-2007-V-1-ABEYAGUNAWARDANE-v.-SAMOON-AND-OTHERS.pdf>
- Abu Bakr v. The Queen*, 54 N.L.R. 566 (1953). <https://lankalaw.net/wp-content/uploads/2024/12/140-NLR-NLR-V-54-M.-S.-ABU-BAKR-Appellant-and-THE-QUEEN-Respondent.pdf>
- Akshay Hari Om Bhatia v. John Doe*, IA(L) No. 33184 of 2025 (Bombay High Court, 2025). <https://indiankanoon.org/doc/60667097/>
- Akshay Tanna v. John Doe*, CS(COMM) 92/2024 (Delhi High Court, 2024). <https://indiankanoon.org/doc/198195535/>
- Anil Kapoor v. Simply Life India*, CS(COMM) 652/2023 (Delhi High Court, 2023). <https://indiankanoon.org/doc/113724486/>
- Benwell v. Republic of Sri Lanka*, [1978–1979] 2 Sri L.R. 194. <https://lankalaw.net/wp-content/uploads/2024/12/031-SLLR-SLLR-1978-79-V2-Benwell-v.-Republic-of-Sri-Lanka.pdf>
- Bridges v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058. <https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/>
- Chaitanya Rohilla v. Union of India*, W.P.(C) 15596/2023 (Delhi High Court, 2024). <https://indiankanoon.org/doc/43358219/>
- Coalition for Content Provenance and Authenticity. (2026, April). *C2PA technical specification* (Version 2.4). [https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA Specification.html](https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA%20Specification.html)
- Code of Criminal Procedure Act, No. 15 of 1979 (Sri Lanka). <https://www.srilankalaw.lk/c/217-code-of-criminal-procedure-act.html>
- Computer Crime Act, No. 24 of 2007 (Sri Lanka). <https://www.icta.lk/icta-assets/uploads/2016/03/ComputerCrimesActNo24of2007.pdf>
- Criminal Procedure Rules 2025, pt. 19 (England & Wales). <https://www.gov.uk/guidance/criminal-procedure-rules-2025-and-criminal-practice-directions-2023>
- Crown Prosecution Service. (2023). *Expert evidence*. <https://www.cps.gov.uk/prosecution-guidance/expert-evidence>
- De Vas Gunawardane v. Attorney General*, S.C. TAB Nos. 01A–01F/2017 (Supreme Court of Sri Lanka, 2024). https://supremecourt.lk/wp-content/uploads/judgements/01a_01f_2017_tab.pdf
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, 2016 O.J. (L 119) 89. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>
- Electronic Transactions Act, No. 19 of 2006, as amended by the Electronic Transactions (Amendment) Act, No. 25 of 2017 (Sri Lanka). <https://www.srilankalaw.lk/e/328-electronic-transactions-act.html>
- Evidence Ordinance, No. 14 of 1895 (Cap. 14) (Sri Lanka). <https://www.srilankalaw.lk/revised-statutes/volume-iii/354-evidence-ordinance.html>

- Evidence (Special Provisions) Act, No. 14 of 1995 (Sri Lanka).
<https://www.srilankalaw.lk/revised-statutes/volume-iii/352-evidence-special-provisions-act.html>
- Forensic Science Regulator. (2025, June 5). *Forensic science activities: Statutory code of practice* (Version 2). Home Office. <https://www.gov.uk/government/publications/forensic-science-activities-statutory-code-of-practice-version-2>
- Hameed v. State by Bidadi Police*, Criminal Petition No. 10135 of 2025 (Karnataka High Court, 2025). <https://indiankanoon.org/doc/127416580/>
- Home Office. (2023). *Extraction of information from electronic devices: Code of practice*. <https://www.gov.uk/government/consultations/extraction-of-information-from-electronic-devices-code-of-practice/extraction-of-information-from-electronic-devices-code-of-practice-accessible>
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-86>
- Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In *Proceedings of the Conference on Fairness, Accountability, and Transparency* (pp. 220–229). Association for Computing Machinery. <https://doi.org/10.1145/3287560.3287596>
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). <https://doi.org/10.6028/NIST.AI.100-1>
- National Stock Exchange of India Ltd. v. Meta Platforms Inc.*, Interim Application (L) No. 21456 of 2024 in Commercial IPR Suit (L) No. 21111 of 2024 (Bombay High Court, 2024). <https://indiankanoon.org/doc/156122165/>
- Phillips, P. J., Hahn, C. A., Fontana, P. C., Yates, A. N., Greene, K., Broniatowski, D. A., & Przybocki, M. A. (2021). *Four principles of explainable artificial intelligence* (NISTIR 8312). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8312>
- Police and Criminal Evidence Act 1984, c. 60 (UK).
<https://www.legislation.gov.uk/ukpga/1984/60>
- R. v. Bater-James*, [2020] EWCA Crim 790.
<https://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html>
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689) 1. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Scientific Working Group on Digital Evidence. (2024, February 2). *Best practices for personnel presenting digital evidence in legal proceedings* (SWGDE 23-Q-001-1.1). <https://www.swgde.org/documents/published-complete-listing/23-q-001-best-practices-for-personnel-presenting-digital-evidence-in-legal-proceedings/>
- Scientific Working Group on Digital Evidence. (2025, November 20). *Best practices for digital evidence collection* (SWGDE 18-F-002-2.0). <https://www.swgde.org/documents/published-complete-listing/18-f-002-2-0/>