International Journal of Innovative Inventions in Social Science and Humanities

ISSN(print): 3050-6921, ISSN(online): 3050-693X

Volume 03 Issue 11 November 2026

DOI: 10.58806/ijiissh.2026.v3i11n11

Page No: 1625-1641

Digital Evidence and the Integrity of Adjudication in Ghana: Authentication, Synthetic Media and Procedural Fairness

Dr Godwin Gaduga

Lecturer at Accra Institute of Technology Adjunct Lecturer at Blue Crest University College.

ABSTRACT

This article contends that the arrival of synthetic media in Ghanaian litigation presents a problem of adjudicative integrity which the law of admissibility, taken alone, cannot resolve. The Evidence Act, 1975 (NRCD 323) sets a deliberately modest threshold of authentication, and section 7 of the Electronic Transactions Act, 2008 (Act 772) relocates questions of generation, storage, integrity and attribution from the threshold of admission to the assessment of weight. That settlement presupposes two conditions: that the ordinary modes of authentication, which rest upon human recognition, are reasonably reliable indicators of genuineness, and that the opposing party has a realistic means of testing what the threshold admits. Generative technologies erode the first condition by manufacturing artefacts designed to be recognized, and they aggravate the unequal distribution of the second by raising the cost of forensic contestation. The article therefore moves the analysis from admissibility to the guarantee of a fair hearing in article 19 of the 1992 Constitution, and argues that the decisive question is how the capacity to test a contested exhibit is distributed between the parties and supplemented by the court. Three contributions follow. The first is a credible challenge procedure, available within the existing provisions of the Evidence Act on the evidential burden and preliminary facts, under which a particularized allegation of fabrication moves the evidential burden back to the proponent while a bare assertion does not; the procedure guards at once against the admission of fabricated records and against the strategic disbelief of genuine ones. The second is an account of custody as proof, which treats the security duties imposed by data protection and cybersecurity law upon the custodians of digital records, including the Judiciary under its E-Justice Plus programme, as evidential guarantees of integrity. The third is a statement of the conditions on which machine assessments of authenticity may inform judicial evaluation without displacing it. Throughout, the article distinguishes requirements confirmed in enacted law from measures announced but not yet binding and from safeguards proposed here, and it identifies the evidence by which their implementation could be evaluated. Public procurement, the contractual allocation of responsibility and the general remedies for automated decision-making, which the author examines in two companion articles, are addressed only so far as they bear upon proof.

KEYWORDS: Authentication, Synthetic Media, Deepfakes, Procedural Fairness, Article 19, Electronic Transactions Act, Chain Of Custody, Liar's Dividend, Ghana

ARTICLE DETAILS

Published On:
16 November 2026

Available on:
https://ijiissh.com/

I. INTRODUCTION

Every adjudication rests upon a premise so elementary that it is seldom stated: that the record placed before the tribunal bears a reliable relationship to the events it purports to describe. The law of evidence has never supposed that premise to be secure. Witnesses lie, instruments are forged, and photographs are retouched, and much of the apparatus of proof, from the oath and cross-examination to the rules on hearsay and authentication, exists to manage the risk that the record and the world have come apart. What is new is the ease of falsification. It has become inexpensive, rapid, available to persons without technical training and capable of producing artefacts that defeat unaided human perception. A voice note in which a company director appears to authorise a transfer, a video in which a public officer appears to accept payment, a screenshot of a mobile money transaction that never occurred:

each may now be generated within minutes, and each may be tendered in a Ghanaian court through the same procedural channels that carry genuine records.

The danger runs in two directions, and the difficulty of the problem lies in their conjunction. The first is the familiar risk that a fabricated record will be accepted as genuine, so that a person is convicted, held liable or deprived of property on the strength of an event that did not happen. The second, which Chesney and Citron have called the liar's dividend, is that the mere availability of fabrication supplies a ready answer to inconvenient proof, so that genuine evidence is discounted because it might have been manufactured.[1] Both failures corrupt the factual foundation of judgment, and both fall more heavily upon the party with fewer resources. The means of testing a digital record, namely access to native files and metadata, to devices and platform records, and to qualified forensic examination, are distributed as unequally as wealth and institutional position. Damaška's observation that the law of evidence was built upon assumptions about the fact-finder and the trial which modern conditions have steadily unsettled applies here with particular force, because the assumption now in question is the reliability of perception itself.[2]

The central claim of this article is that synthetic media confront Ghana with a problem of adjudicative integrity that the law of admissibility cannot resolve on its own. Section 7 of Act 772 deliberately moved the questions of reliability, integrity and attribution from the threshold of admission to the assessment of weight, and that choice remains defensible as a matter of evidentiary policy. A weight-based model works, however, only where the tribunal has the means of assessing weight, and those means increasingly lie outside the courtroom: in the forensic capacity of investigative institutions, in the retention and disclosure practices of platforms and telecommunications operators and, since the Judiciary adopted electronic filing, authentication and service, in the integrity of the court's own systems. The soundness of a judgment that rests upon a digital exhibit therefore depends upon the reasoning of the trial judge and also upon conditions of custody and contestation that precede and surround the trial.

The article stands in a deliberate relationship to two companion studies by the author. The first examines the governance of the public acquisition of artificial intelligence, including procurement law, the contractual allocation of responsibility, and data sovereignty. The second examines the remedies available to persons affected by AI-assisted decisions, including the operation of section 41 of the Data Protection Act, 2012 (Act 843) and the demands of algorithmic transparency and human review.[3] Those questions are not revisited here. This article is confined to the distinct question of proof: how Ghanaian courts should authenticate, test and evaluate digital records when convincing fabrication is commonplace, and what institutional conditions must exist for that evaluation to be fair. It also builds upon, without restating, the author's earlier proposals of a sequence of judicial questions for electronic evidence and of a chain of provenance as the successor to the chain of custody.[4]

The argument proceeds in ten further Parts. Part II sets out the evidential framework and identifies the premises on which it rests. Part III examines the authentication rule, locates the points at which recognition-based authentication fails, and proposes a credible challenge procedure. Part IV treats synthetic media as an epistemic rather than a merely technical phenomenon. Part V takes the fair hearing guarantee as the organizing principle for distributing the capacity to test. Part VI develops the account of custody as proof. Part VII states the conditions on which machine assessments of authenticity may inform judicial evaluation. Part VIII considers the correction of judgments later found to rest upon fabricated records. Parts IX and X distinguish confirmed requirements from announced and proposed measures and identify the evidence needed to evaluate implementation, and Part XI concludes. Statements of Ghanaian law are made as at 30 October 2026.

II. THE EVIDENTIAL FRAMEWORK AND ITS PREMISES

No Ghanaian enactment yet addresses the evidential treatment of synthetic media. The governing law must be assembled from constitutional guarantees, the general law of evidence, the special regime for electronic records and the rules of court, each of which was framed with other risks in view. This Part does not survey those instruments exhaustively. Its purpose is to identify the premises on which their combined operation depends, since those are the premises that synthetic media call into question.

[1]Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, 1785.

[2]Mirjan R Damaška, *Evidence Law Adrift* (Yale University Press 1997).

[3]Godwin E K Djokoto, 'Governing the Public-Sector Acquisition of Artificial Intelligence in Ghana: Data Sovereignty, Human Accountability and the Limits of Technical Oversight' (2026, forthcoming); Godwin E K Djokoto, 'From Data Protection to Algorithmic Accountability: Rethinking Legal Remedies for AI-Assisted Decisions in Ghana' (2026, forthcoming).

[4]Godwin E K Djokoto, 'Judicial Standards for Electronic Evidence in Ghana: Building a Coherent Jurisprudence for the Digital Age' (2026, forthcoming); Godwin E K Djokoto, *The Manufactured Fact: Truth, Authenticity and Legal Proof in Ghana's Synthetic Information Age* (forthcoming).

A. The constitutional standard

Article 19 of the Constitution secures a fair hearing within a reasonable time before an independent and impartial court, and in criminal proceedings it guarantees to the accused adequate time and facilities for the preparation of a defence and facilities to examine the witnesses called by the prosecution.[5] Article 18(2) protects the privacy of correspondence and communication, and so conditions the manner in which digital records are obtained, retained and disclosed.[6] Article 125 vests judicial power in the Judiciary and places its administration under the Chief Justice, while article 12 binds the Judiciary, together with the Executive and the Legislature, to respect and uphold the fundamental rights in Chapter Five.[7] Read together, these provisions make the fairness of adjudication a constitutional value, and they place upon the Judiciary responsibility for the conditions, technological conditions included, under which it adjudicates.

B. The general law of authentication

Section 136 of the Evidence Act provides that where the relevance of evidence depends upon its authenticity or identity, the requirement of authentication is satisfied by evidence or other showing sufficient to support a finding that the matter in question is what its proponent claims.[8] Sections 137 to 142 illustrate the means by which that showing may be made, including the testimony of a witness with knowledge, non-expert opinion on handwriting, comparison by the court or a witness, and voice identification.[9] The Act distinguishes carefully between the burden of producing evidence, which may pass between the parties as a case develops, and the burden of persuasion, and it permits the exclusion of relevant evidence whose probative value is substantially outweighed by the risk of unfair prejudice or of misleading the tribunal.[10] Two premises are embedded in this scheme. The first is that the illustrative modes of authentication, which rest largely upon human recognition, are reasonably reliable indicators of genuineness. The second is that adversarial testing at the stage of weight will detect what a low threshold admits.

C. The special regime for electronic records

Act 772 treats the integrity of an electronic record as a question of whether it has remained complete and unaltered, apart from changes arising in the normal course of communication, storage and display, and section 7(1) provides that the rules of evidence shall not be applied to deny admissibility merely because a record is electronic.[11] Section 7(2) directs the court, in assessing weight, to the reliability of the manner in which the record was generated, stored or communicated, the reliability of the manner in which its integrity was maintained, and the manner in which its originator was identified.[12] The section names the matters to be weighed. It does not say who must establish them, to what standard, or with what access to the underlying systems, and that silence is the central doctrinal gap examined in Part III. A draft Electronic Transactions Bill, 2025, which would repeal Act 772, has been published for consultation but has not been enacted.[13]

D. The court as producer of electronic records

The High Court (Civil Procedure) Rules, 2004 were amended in 2019 to provide for electronic service of process.[14] On 29 July 2026 the Chief Justice announced that electronic filing, electronic authentication and electronic service of court processes would become the standard from 1 October 2026 under the E-Justice Plus agenda, that automation would proceed in stages beginning with the Supreme Court, and that revised Rules of Court would be laid before Parliament at the opening of the legal year.[15] At the time of writing the revised Rules had not, so far as could be established, completed their passage. The significance of these developments is that the courts have become producers and custodians of electronic records on a scale that makes the integrity of their own systems an evidential question. Act 843 and the Cybersecurity Act, 2020 (Act 1038) bear upon that question by imposing security duties

[5]Constitution of the Republic of Ghana 1992, art 19(1), (2)(e), (2)(g) and (13).

[6]ibid art 18(2).

[7]ibid arts 12(1) and 125(1), (3) and (4).

[8]Evidence Act 1975 (NRCD 323), s 136.

[9]ibid ss 137 to 142.

[10]ibid ss 10 to 17, 51 and 52.

[11]Electronic Transactions Act 2008 (Act 772), ss 6 and 7(1).

[12]ibid s 7(2).

[13]Electronic Transactions Bill 2025 (consultation draft); LEX Africa, 'E-Signed, Sealed and Delivered: Ghana's Current Legal Framework and Proposed Reforms for E-Signatures' (July 2026) <https://lexafrica.com/2026/07/ghanas-current-legal-framework-and-proposed-reforms-for-e-signatures/> accessed 30 October 2026.

[14]High Court (Civil Procedure) Rules 2004 (CI 47), Ord 7 r 3A, inserted by the High Court (Civil Procedure) (Amendment) Rules 2019 (CI 122).

[15]Ghana News Agency, 'Judiciary to Roll Out Electronic Court Processes from October: CJ' (29 July 2026) <https://gna.org.gh/2026/07/judiciary-to-roll-out-electronic-court-processes-from-october-cj/> accessed 30 October 2026.

upon the custodians of personal data and of critical information infrastructure, and Part VI considers those duties in their evidential aspect only.[16]

E. Pending reform and the present gap

Several bills bearing upon digital governance, among them a Data Protection Bill, a Cybersecurity (Amendment) Bill and an Emerging Technologies Bill, have been published or announced. None is law, and none, in the drafts publicly available, addresses the evidential use of synthetic records.[17] Prosecutions arising from AI-generated impersonation of public figures were reported before the Accra courts during 2026, which shows that the problem is no longer prospective.[18] What the framework lacks is a coherent allocation of the burdens, costs and institutional responsibilities that synthetic media impose upon proof; a rule that merely names deepfakes would not supply it.

III. AUTHENTICATION AND THE EXHAUSTION OF RECOGNITION

Authentication in Ghanaian law is a threshold of sufficiency, not a finding of genuineness. The distinction serves adjudication well where the risk is the isolated forgery. It becomes a structural weakness where the risk is a class of artefacts engineered to satisfy exactly the kind of evidence that the threshold accepts.

A. The logic of the sufficiency threshold

Section 136 does not require the judge to find that an item is genuine. It requires the judge to find that a reasonable tribunal could so find, after which the question of genuineness passes to the assessment of weight on the whole of the evidence.[19] The formulation derives from the American model codified in Federal Rule of Evidence 901(a), and its rationale is the same. Authentication is a question of conditional relevance, and to require the proponent to prove genuineness on the balance of probabilities before the item can be heard would invert the ordinary sequence of trial and draw the judge into a function that belongs to the tribunal of fact.[20] Section 7 of Act 772 is consistent with that design: it removes electronic form as a ground of exclusion and directs scrutiny of generation, storage and integrity to the stage of weight. The author has argued elsewhere that the placement of the section 7(2) factors under weight confirms that the authentication threshold for electronic records remains one of sufficiency, and the present analysis does not disturb that reading.[21]

B. The premises exposed

A low threshold is defensible only while the two premises identified in Part II hold, and synthetic media undermine both. The modes of authentication illustrated in sections 139 to 142 of the Evidence Act rely upon recognition: a witness with knowledge attests that a photograph fairly depicts a scene, a person familiar with a voice identifies it, or the court compares a disputed item with an exemplar.[22] A generative system trained or prompted to reproduce a particular face or voice produces an artefact whose whole purpose is to be recognized. The witness who honestly identifies a director's voice in a fabricated recording therefore satisfies the statutory illustration while being deceived by it. Recognition has ceased to be independent evidence of genuineness in precisely the cases in which genuineness is in doubt. At the stage of weight, the factors in section 7(2) concern the reliability of systems, the maintenance of integrity and the identification of originators, and each can be assessed only with access to native files, metadata, device extractions, platform records or expert examination. None of these lies within the ordinary reach of a litigant without the assistance of the court.

C. Three doctrinal gaps

The existing law fails at three identifiable points. The first is the incidence of proof on the section 7(2) factors. The statute prescribes what is to be considered but not who must establish it, and in practice the factors are often treated as matters for the opponent to disprove. That approach quietly converts an inquiry into weight into a presumption of reliability in favour of whatever system

[16]Data Protection Act 2012 (Act 843), ss 17 and 91; Cybersecurity Act 2020 (Act 1038).

[17]Kofi Anokye Owusu-Darko, 'The Data Protection Bill 2025: A Stronger Shield' *Business & Financial Times* (Accra, 20 May 2026) <https://thebftonline.com/2026/05/20/the-data-protection-bill-2025-a-stronger-shield-what-is-it-meant-to-enable/> accessed 30 October 2026; Cyber Security Authority, 'Public Consultation on the Draft Cybersecurity (Amendment) Bill, 2025' <https://csa.gov.gh/public_document.php> accessed 30 October 2026; 'Gov't to Lay Emerging Technologies Bill before Parliament in 2026' *Citi Newsroom* (Accra, 5 November 2025) <https://www.citinewsroom.com/2025/11/govt-to-lay-emerging-technologies-bill-before-parliament-in-2026/> accessed 30 October 2026.

[18]'The Rise of AI Deepfake Fraud in Ghana: Inside the Accra High Court Case' *Modern Ghana* (17 June 2026) <https://www.modernghana.com/blogs/1503245/the-rise-of-ai-deepfake-fraud-in-ghana-inside.html> accessed 30 October 2026.

[19]NRCD 323, s 136.

[20]Federal Rules of Evidence (US), rr 104(b) and 901(a), and the Advisory Committee Note to r 901.

[21]Djokoto, 'Judicial Standards for Electronic Evidence in Ghana' (n 4).

[22]NRCD 323, ss 139 to 142.

generated the record. The second is the consequence of a challenge. Neither the Evidence Act nor Act 772 says what follows when an opponent raises a credible allegation of fabrication or material alteration. Courts are left to choose between disregarding the allegation, which rewards fabrication, and treating any allegation as decisive, which rewards the liar's dividend. The third is access. The law gives the proponent the benefit of a low threshold without giving the opponent any corresponding entitlement to the materials without which the section 7(2) factors cannot be contested.

D. Comparative experience

Comparative experience shows that these gaps are widely recognized and have nowhere yet been closed. The United States Advisory Committee on Evidence Rules, after three years of study, drafted and held in reserve a proposed Rule 901(c), under which a sufficient showing of fabrication would require the proponent to establish authenticity on the balance of probabilities. In May 2026, it declined to recommend either that text or the separate proposed Rule 707 on machine-generated evidence, and deferred both to further consultation in October 2026.[23] Its hesitation rested partly on empirical grounds: a Federal Judicial Center survey found that only fifteen of 931 responding judges had encountered a challenge to evidence as a deepfake.[24] In England and Wales, the common law presumption that computers operate correctly, applied with grave consequences in the prosecutions founded upon the Horizon accounting system, has been the subject of a governmental call for evidence but not of enacted reform.[25] Singapore retains statutory presumptions for electronic records and India a certification requirement.[26] None of these models should simply be transplanted. What they show is that each jurisdiction has found it necessary to say something about the burden and its consequences once a challenge is made, and that the gravest failure, Horizon, arose from an unexamined assumption of reliability combined with the non-disclosure of known defects rather than from fabrication.

E. A credible challenge procedure within existing law

The first two gaps can largely be addressed without legislation. The Evidence Act already distinguishes the evidential burden, which may move in the course of a case, from the burden of persuasion, and already commits to the court the determination of preliminary facts on which admissibility depends.[27] The procedure proposed here is a safeguard for judicial adoption; it does not describe existing practice. It has four stages. First, the proponent satisfies section 136 ordinarily. Second, an opponent who alleges fabrication or material alteration must make a particularized showing that goes beyond bare assertion, whether by pointing to an inconsistency in metadata, the absence of an original on the device from which the item is said to come, an expert observation, an alibi irreconcilable with the depicted event, or some comparable foundation on which a reasonable tribunal could find fabrication. Third, once such a showing is made, the evidential burden passes back to the proponent to adduce evidence directed to the section 7(2) factors, including the native file, its provenance and the chain by which it reached the court, and the court may give directions for disclosure, inspection or examination by an expert of its own appointment. Fourth, the court determines the challenge by a reasoned ruling that records the foundation of the challenge, the evidence adduced in answer, and the reasons for admission, exclusion or admission subject to directions as to weight.

The procedure deliberately stops short of the reserved American text, which would shift the burden of persuasion on authenticity for every challenged item. Such a change would alter a standing allocation of the burden of proof and is, on the better view, a matter for Parliament or the Rules of Court Committee rather than for incremental judicial development.[28] What the courts can do now is govern the movement of the evidential burden, the scope of disclosure and the appointment of experts, and those powers are sufficient to remedy most of the practical injustice that the gaps produce. Figure 1 sets out the procedure; the branch at the second stage marks the distinction between a particularized challenge and a bare assertion.

[23] Advisory Committee on Evidence Rules, *Agenda Book* (May 2026) pt IV <https://www.uscourts.gov/sites/default/files/document/advisory_committee_on_evidence_rules_may_2026.pdf> accessed 30 October 2026.

[24] Federal Judicial Center survey (March 2026), reported in 'AI Deepfakes Put Courtroom Evidence Under Growing Cloud of Doubt' *Court Cast* (16 October 2026) <https://courtscast.com/ai-deepfakes-put-courtroom-evidence-under-growing-cloud-of-doubt-openai-and-meta-warn/> accessed 30 October 2026.

[25] *Bates v Post Office Ltd (No 6: Horizon Issues)* [2019] EWHC 3408 (QB); *Hamilton v Post Office Ltd* [2021] EWCA Crim 577; Ministry of Justice, *Use of Evidence Generated by Software in Criminal Proceedings: Call for Evidence* (21 January 2025).

[26] Evidence Act 1893 (Singapore), s 116A; *Gil v Public Prosecutor* [2025] SGCA 21; Bharatiya Sakshya Adhiniyam 2023 (India), s 63.

[27] NRCD 323, ss 1 to 4 and 10 to 17.

[28] Djokoto, *The Manufactured Fact* (n 4).

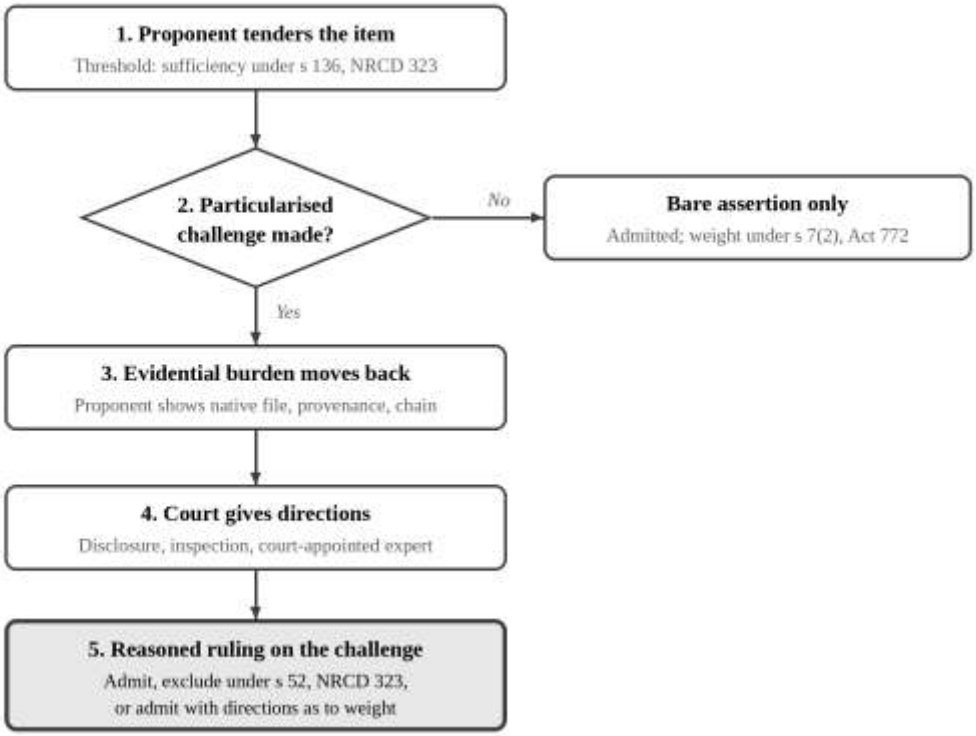

Figure 1. **The proposed credible challenge procedure. A bare assertion of fabrication leaves the item to the ordinary assessment of weight; only a particularized showing moves the evidential burden and engages the court's powers of direction.**

IV. SYNTHETIC MEDIA AND THE EPISTEMOLOGY OF ADJUDICATION

Synthetic media are better understood as a change in the economics of doubt than as a new species of forgery. They reduce the cost of fabricating a convincing record, and in doing so they also reduce the cost of disbelieving a genuine one.

A. Four evidential situations

The term 'deepfake' conceals four situations that the law should keep apart, because each raises a different question and calls for a different response. The first is the wholly synthetic record, generated without any underlying event. The second is the manipulated authentic record, in which a genuine recording or document has been altered in a material respect. The third is the authentic but decontextualized record: a genuine item presented with a false date, place, speaker or purpose. It requires no artificial intelligence at all and remains in practice the commonest form of digital deception. The fourth is the authentic record falsely impugned as synthetic, where the evidential difficulty lies in the challenge rather than in the item.[29] A court that treats these as a single phenomenon will apply forensic techniques designed for the first two to disputes that turn upon the third, and will be exposed to the fourth whenever it gives weight to an unparticularized suggestion of fabrication.

B. Adjudicative truth as warranted belief

The deeper significance of synthetic media lies in what they reveal about adjudicative fact-finding. Wiredu's account of truth as opinion treats truth as the considered judgment of a point of view warranted by the evidence available to it, rather than as a correspondence apprehended directly, and it offers a useful frame for judicial findings of fact.[30] A court never perceives the past event. It forms a warranted belief about that event on the basis of a record, and the legitimacy of its finding depends upon the quality of the warrant. On this view, synthetic media do not make truth unknowable, which in the relevant sense it always was. They degrade the warrant that certain kinds of record have traditionally supplied. The photograph and the recording carried a high warrant because their production was causally tied to the event they depicted. Generative technologies sever that tie while preserving the appearance

[29]Chesney and Citron (n 1); Rebecca A Delfino, 'Deepfakes on Trial: A Call to Expand the Trial Judge's Gatekeeping Role to Protect Legal Proceedings from Technological Fakery' (2023) 74 Hastings Law Journal 293.

[30]Kwasi Wiredu, 'Truth as Opinion' in Kwasi Wiredu, *Philosophy and an African Culture* (Cambridge University Press 1980).

of the record, so that the warrant a court may draw from appearance alone diminishes. The adjudicative task accordingly shifts from evaluating what a record shows to evaluating how the record came to exist: from content to provenance.

C. The threat to the integrity of adjudication

The integrity of adjudication depends upon three conditions: that the tribunal decides upon a record that is what it purports to be; that each party has a fair opportunity to test that record; and that the tribunal's reasons disclose how the record was evaluated. Synthetic media endanger each condition differently. They endanger the first directly, since a fabricated exhibit corrupts the factual premise of judgment however sound the reasoning built upon it. They endanger the second indirectly, since the capacity to test a digital record is unequally distributed and its cost rises as fabrication becomes more sophisticated. They endanger the third because a judge who cannot explain why one expert's assessment of a recording is preferred to another's produces a finding that cannot be reviewed on appeal. The effect is also systemic. If litigants come to believe that recordings can be fabricated at will and that courts cannot tell the difference, parties with weak cases are encouraged to manufacture evidence and parties faced with strong evidence are encouraged to deny it. The liar's dividend may then be collected without any fabrication having occurred.[31]

D. The limits of detection and the turn to provenance

It is tempting to suppose that the answer to generative technology is detection technology. The supposition is unsafe. Detection tools are probabilistic classifiers whose outputs express likelihood, not findings. Their error rates vary with the generator, the quality of the original and the compression applied in transmission, and recordings that have passed through messaging services, which describe much of the audio and video tendered in Ghanaian courts, are routinely recompressed in ways that destroy the artefacts on which many detectors depend. Detection is also adversarial, since generators improve in response to detectors.[32] The more durable response, now being built into some devices and platforms, is provenance: cryptographically signed content credentials recording how an item was captured and edited, of the kind specified by the Coalition for Content Provenance and Authenticity.[33] Provenance has limits of its own. Its absence proves nothing, and most devices in use in Ghana do not yet generate it. It nonetheless changes the inquiry from whether an item appears fabricated to whether its history can be shown, and that is the inquiry the section 7(2) factors of Act 772 are already built to accommodate.

E. Upstream regulation and its absence

Other legal orders have begun to regulate synthetic media at the point of production. The European Union's Artificial Intelligence Act requires providers of generative systems to mark outputs in machine-readable form and requires deployers of systems that produce deepfakes to disclose their artificial character; these obligations apply in principle from 2 August 2026.[34] Ghana has no equivalent enacted obligation. The pending Emerging Technologies Bill and Data Protection Bill have been publicly associated with the regulation of misinformation and deepfakes, but neither is law and neither, in the drafts available, deals with evidential use.[35] The offence in Act 1038 of distributing intimate images without consent will increasingly reach synthetic imagery, and it bears upon how such material is handled once it becomes an exhibit.[36] Ghanaian courts therefore cannot rely upon upstream labelling to identify synthetic content. They must develop their own responses, calibrated to the four situations identified above: provenance evidence for the first and second, contextual corroboration for the third, and a firm insistence upon particularization for the fourth. The chain of provenance, which the author has proposed as the successor to the traditional chain of custody, is directed to precisely this change of focus.[37]

[31] Chesney and Citron (n 1) 1785 to 1786.

[32] Riana Pfefferkorn, '"Deepfakes" in the Courtroom' (2020) 29 Boston University Public Interest Law Journal 245.

[33] Coalition for Content Provenance and Authenticity, *C2PA Technical Specification* <https://c2pa.org/specifications/> accessed 30 October 2026.

[34] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, arts 50(2), 50(4) and 113.

[35] Africa Policy and Development Institute, 'Emerging Technologies Bill' <https://apdigh.org/bills/2-emerging-technologies-bill/> accessed 30 October 2026; 'Ghana's AI and Deepfake Rules: What the New Data Protection Bill Means' *Wansom* (22 October 2026) <https://www.wansom.ai/briefly/news/ghana-s-ai-and-deepfake-rules-what-the-new-data-protection-bill-means-2026-10-22> accessed 30 October 2026.

[36] Act 1038, provision on the non-consensual sharing of intimate images.

[37] Djokoto, *The Manufactured Fact* (n 4).

V. PROCEDURAL FAIRNESS AND THE DISTRIBUTION OF THE CAPACITY TO TEST

The injustice that synthetic media create lies less in the admission of a particular exhibit than in the inequality of the parties' capacity to examine it. If that is right, the governing standard must be found in the constitutional guarantee of a fair hearing, which is concerned with the conditions under which each party is enabled to answer the case against it, rather than in the law of admissibility.

A. From admissibility to fair opportunity

A merely formal opportunity to be heard has never satisfied the fair hearing guarantee. In criminal proceedings article 19 secures adequate time and facilities for the preparation of a defence and facilities to examine the witnesses called by the prosecution.[38] The Supreme Court has read those guarantees as requiring pre-trial disclosure to the accused of the material on which the prosecution intends to rely, and the Chief Justice has since issued a practice direction on disclosure and case management in criminal proceedings.[39] The logic of those developments extends naturally to digital records, and the extension exposes a distinction that current practice tends to obscure. Disclosure of a screenshot is not disclosure of the record the screenshot depicts. Disclosure of a transcript is not disclosure of the audio from which it was made. A forensic report that states a conclusion without its method, instrument, version, settings, and hash values does not disclose the means of testing that conclusion. A fair opportunity to examine a contested digital exhibit requires access to the native file and its metadata, to the extraction from which it was taken, and to enough information about any processing it has undergone to permit independent examination.

Civil proceedings raise the same question in another form. The rules on discovery and inspection in the High Court (Civil Procedure) Rules, 2004 were framed for documents on paper and have been extended to electronic material by analogy. They do not specify the form in which electronic documents must be produced, so a party who produces a printout of an email instead of the native message withholds, without breaching the letter of the rules, the very metadata from which authenticity might be assessed.[40] The principle of equality of arms, which the European Court of Human Rights treats as inherent in a fair hearing in civil as well as criminal matters, supplies a persuasive interpretive standard: each party must have a reasonable opportunity to present its case under conditions that do not place it at a substantial disadvantage in relation to its opponent.[41]

B. The cost of contestation

The most acute difficulty is cost. Forensic examination of audio and video demands specialist expertise and instruments, and frequently access to the device or account of origin. In criminal matters, the prosecution ordinarily has recourse to the forensic laboratories of the investigative agencies, while the accused has no comparable resource; in civil matters, the asymmetry tracks wealth. The Evidence Act already empowers the court to appoint its own expert, whose report is admissible to the same extent as that of any other expert witness, and the Legal Aid Commission Act, 2018 (Act 977) provides a framework for publicly funded assistance.[42] Neither was designed with forensic digital examination in mind. The proposal advanced here is that, where a party who cannot reasonably fund an examination raises a particularized challenge under the procedure described in Part III, the court should treat the appointment of its own expert as the presumptive response rather than an exceptional indulgence, at public expense in criminal proceedings and with costs reserved in civil proceedings. The proposal has fiscal implications and would need institutional support. It is not at present a requirement of Ghanaian law.

C. Fairness in both directions

Procedural fairness protects both sides, and an account of it that attends only to the accused or the defendant is incomplete. A complainant whose genuine recording of threats or abuse is met with an unsupported allegation of fabrication is equally entitled to have the recording assessed on its merits. The credible challenge procedure protects both interests by requiring particularization before the evidential burden moves. It also implies a duty of candour. A legal practitioner who suggests that evidence is synthetic without a proper foundation risk misleading the court, and the professional conduct rules that forbid practitioners from knowingly misleading the court should be understood to reach that conduct. Equally, a practitioner who tenders an item while having reason to believe it has been altered or generated assumes responsibility for it.[43]

[38] Constitution, art 19(2)(e) and (g).

[39] *Republic v Eugene Baffoe-Bonnie and Four Others* (Supreme Court); Practice Direction (Disclosures and Case Management in Criminal Proceedings) 2018.

[40] CI 47, Ord 21.

[41] *Dombo Beheer BV v Netherlands* (1994) 18 EHRR 213, para 33.

[42] NRCD 323, provisions on court-appointed experts; Legal Aid Commission Act 2018 (Act 977).

[43] Legal Profession (Professional Conduct and Etiquette) Rules 2020 (LI 2423).

D. The unrepresented litigant and the inquisitorial supplement

A large proportion of litigants in the District and Circuit Courts appear without counsel, and they are the least able to recognise when a digital exhibit should be challenged or to frame a particularized challenge. A purely adversarial model of testing will fail such litigants systematically, because it presupposes a capacity to interrogate provenance that they do not have. The fair hearing guarantee supports a modest inquisitorial supplement. Where an unrepresented party disputes a recording, the court should itself put the elementary questions of provenance that the party cannot formulate: where the original is, on what device it was made, by what route it reached the court, and whether anyone has examined it. The supplement imposes no new burden of proof. It is an exercise of the court's ordinary duty to secure a fair hearing, and it is the one safeguard in this article that needs neither legislation nor public expenditure.

E. Reasons as a condition of fairness

Finally, fairness requires the court to explain how it resolved any contest over a digital exhibit. A ruling that merely records that an exhibit was admitted or found reliable deprives the unsuccessful party of an effective appeal and deprives the legal order of the reasoned decisions from which doctrine develops. The reasoned evidentiary ruling, which the author has proposed as a standard of decision for electronic evidence generally, matters most where synthesis is alleged, because an appellate court can review reasoning about provenance but cannot perceive the recording again as the trial judge perceived it.[44]

VI. CUSTODY AS PROOF

Data protection and cybersecurity law are usually discussed as constraints upon the gathering of evidence. They are also, though this is less often recognized, guarantees of its integrity, because the duties they impose upon the custodians of digital records are the duties on which a court relies when it asks whether a record has remained complete and unaltered. This Part develops that proposition in its evidential aspect only. The governance of the acquisition of the systems in which records are held, and the contractual allocation of responsibility for their performance, are treated in the author's companion study and are not revisited here.[45]

A. The convergence of integrity duties

Act 843 applies to the state, treats each government department as a data controller, and requires that personal data be protected by appropriate and reasonable technical and organizational measures against loss, unauthorized alteration and unlawful access.[46] Section 6 of Act 772 defines the integrity of an electronic record by reference to whether it has remained complete and unaltered.[47] The two provisions converge upon a single question. A court assessing weight under section 7(2) of Act 772 asks about the reliability of the manner in which a record's integrity was maintained. A custodian that has discharged its security obligations by restricting access, logging alterations and preserving originals will be able to answer that question; a custodian that has not will be unable to do so. The Data Protection Commission's published guidance identifies security safeguards, breach notification and impact assessment for new technologies as core components of compliance.[48] Compliance is therefore more than a matter between the custodian and the Commission. It is evidence of reliability, and its absence is evidence of unreliability. The safeguard proposed here is that a court faced with a particularized challenge to a digital exhibit should be prepared to require the custodian, public or private, to describe the security measures applied to the record, and should treat an inability to do so as bearing directly upon weight.

B. The court's own record

The adoption of electronic filing, authentication and service from 1 October 2026 makes the court's own record a potential object of contest. An intrusion into a case management system could alter a filed exhibit, substitute a process, erase a record of service or manipulate the recording of proceedings, and each would corrupt adjudication from within. Act 1038 provides for the designation and protection of critical information infrastructure, and the Cyber Security Authority has issued a directive on such infrastructure together with a risk assessment framework and a national policy and strategy.[49] Whether any system of the Judiciary has been so designated is not apparent from public sources; Part X accordingly treats it as a matter for evidence rather than assumption. What can be said with confidence is that the authenticity of an electronically authenticated court process depends upon the security of the

[44]Djokoto, 'Judicial Standards for Electronic Evidence in Ghana' (n 4).

[45]Djokoto, 'Governing the Public-Sector Acquisition of Artificial Intelligence in Ghana' (n 3).

[46]Act 843, ss 17, 28 and 91.

[47]Act 772, s 6.

[48]Data Protection Commission, 'Compliance' <https://dpc.gov.gh/compliance/> accessed 30 October 2026; Data Protection Commission, *Guidelines to Demonstrate Data Protection Compliance* (2025).

[49]Act 1038, provisions on critical information infrastructure; Cyber Security Authority, *Critical Information Infrastructure Directive*, *Risk Assessment Framework* and *National Cybersecurity Policy and Strategy* <https://www.csa.gov.gh/resources.php> accessed 30 October 2026.

credentials, keys and logs on which the authentication rests, and that a litigant who disputes the authenticity of a process must be able to examine the standards by which those materials are governed. The Judiciary cannot be both the custodian of the record and the unexamined guarantor of its integrity.

The Post Office litigation in England and Wales is the cautionary example. The High Court found that the Horizon system had contained bugs, errors and defects capable of generating apparent shortfalls in branch accounts, and the Court of Appeal later quashed convictions on the footing that the reliability of Horizon had been essential to the prosecutions and that the prosecuting institution had failed in its duties of investigation and disclosure.[50] The lesson is evidential. An institution that treats its own system as presumptively reliable, while controlling all information about that system's defects, will in time turn a technical fault into a miscarriage of justice.

C. Personal data within exhibits

Digital exhibits routinely contain the personal data of persons who are not parties, and synthetic media sharpen the difficulty. A fabricated intimate image or recording of a real person is itself a grave intrusion upon that person's privacy and dignity, and its reproduction in a court record or published judgment may repeat the injury. Article 18(2) of the Constitution and the data protection principles of minimality and purpose specification support three handling rules: exhibits containing intimate or highly sensitive content should be held under restricted access; published judgments should describe such content rather than reproduce it; and content found to be fabricated should be retained only for as long as the proceedings and any appeal require. The offence in Act 1038 of distributing intimate images without consent reinforces the principle that the court record must not become a further channel of distribution.[51]

D. Forensic practice

Much of the expert evidence on digital exhibits that reaches Ghanaian courts is produced by investigative agencies or private practitioners. The regime under Act 1038 for licensing cybersecurity service providers and accrediting professionals offers a possible foundation for minimum standards of forensic practice, including documented methodology, validation of instruments, peer review and the preservation of working files. The regime was not framed for forensic evidence, however, and its application to forensic examiners would need to be confirmed against the Authority's licensing categories.[52] The pending Cybersecurity (Amendment) Bill, 2025 would extend the Authority's functions into investigation and data preservation. If it were enacted in that form, the Authority would itself become a producer of digital evidence, and the separation of its regulatory and investigative functions would acquire evidential as well as institutional significance.[53]

VII. MACHINE OPINION ON AUTHENTICITY

When a machine is used to pronounce on whether a record is genuine, its output becomes evidence about evidence. It must be subjected to the disciplines of disclosure, testing and reasoned evaluation that the law applies to opinion, and the judicial decision it informs must remain a judgment rather than the ratification of a score. The broader questions of algorithmic transparency and human oversight in administrative decision-making, and the operation of section 41 of Act 843, are examined in the author's companion study on remedies and are not repeated here.[54] This Part is confined to the use of analytical instruments in determining authenticity.

A. Detection outputs as inferential opinion

A synthetic media detector, a voice comparison system or an image forensic suite does not observe facts. It draws inferences from patterns in data according to methods embedded in its design and training, and its output is therefore in substance an opinion. The concerns that attend expert opinion apply to it in full: the sufficiency of the underlying data, the reliability of the method, and the reliability of the method's application to the item in question. Tribe warned half a century ago that numerical expressions of probability carry an appearance of precision that can overwhelm the less quantifiable evidence beside them, and the warning is pertinent again when a classifier reports that a recording is ninety-four per cent likely to be synthetic.[55] The deferred American proposal for a Rule 707 captures the essential point by subjecting machine-generated evidence offered without an expert to the reliability standards that govern expert testimony; commentators have urged that it be confined to machine-generated inferential

[50] *Bates* (n 25); *Hamilton* (n 25).

[51] Act 1038 (n 36).

[52] Act 1038, provisions on the licensing of cybersecurity service providers and the accreditation of cybersecurity professionals.

[53] Cyber Security Authority (n 17); 'Rethinking the Cybersecurity Amendment Bill' *Business & Financial Times* (Accra, 25 November 2025) <https://thebftonline.com/2025/11/25/rethinking-the-cybersecurity-amendment-bill/> accessed 30 October 2026.

[54] Djokoto, 'From Data Protection to Algorithmic Accountability' (n 3).

[55] Laurence H Tribe, 'Trial by Mathematics: Precision and Ritual in the Legal Process' (1971) 84 Harvard Law Review 1329.

evidence, because it is inference, not mechanical recording, that gives rise to the concern.[56] Ghanaian law needs no new rule to reach the same position. The provisions of the Evidence Act on expert opinion, together with the power to exclude evidence whose probative value is substantially outweighed by the risk of misleading the tribunal, already permit a court to require that a detection output be presented through a witness able to explain the method, its validation and its limits, and to give it little or no weight where that cannot be done.[57]

B. The conditions of reliance

The proposal advanced here, as a safeguard rather than an existing requirement, is that a party relying upon the output of an analytical instrument in respect of a contested exhibit should disclose: the identity and version of the instrument; the settings applied; the input actually analyzed, with its hash and a statement whether it was the native file or a copy; the output in full, including any confidence measure; the documented validation of the instrument and its reported error rates; the conditions under which its performance is known to degrade; and the qualifications of its operator. Where disclosure of validation information is refused, the consequence should fall upon the party relying upon the instrument. Experience elsewhere with proprietary risk assessment tools, where courts permitted reliance upon undisclosed methodologies subject only to cautionary advisements, suggests that warnings unaccompanied by access are no substitute for an opportunity to test.[58]

C. Judicial evaluation that remains judicial

Research on automation bias has shown that decision-makers presented with an automated recommendation tend to defer to it, to search less diligently for contrary information, and to overlook errors they would otherwise have detected.[59] A judge presented with an uncontradicted detection score may give it more weight than its validation warrants. Judicial evaluation remains judicial only if three conditions are met. The judge must understand what the output signifies and what it does not, including the difference between a classifier's confidence and the probability that the item was fabricated. The output must be weighed together with the other evidence bearing on authenticity, not in substitution for it. And the reasons given must engage with the output rather than recite it. It follows that no exhibit should be excluded as synthetic, or admitted as genuine over a particularized challenge, on the output of an analytical instrument alone.

VIII. CORRECTING THE RECORD: FABRICATION DISCOVERED AFTER JUDGMENT

The general architecture of remedies for persons harmed by automated or AI-assisted decisions, including regulatory complaint, compensation under Act 843 and constitutional enforcement under articles 23 and 33, is the subject of the author's companion study and is not reconsidered here.[60] This Part addresses a narrower question peculiar to adjudication: what the legal order offers a person who discovers that a judgment against him rested upon a fabricated record, or that a genuine record was wrongly rejected as fabricated. Ghanaian law offers several routes, but each presupposes that the affected person has already discovered the fabrication and can prove it.

A. Before judgment

The most effective correction is the one that precedes judgment. The Evidence Act requires objection to admissibility to be made when the evidence is offered, and the court may determine the objection on a trial within a trial, exclude evidence whose probative value is substantially outweighed by the risk of misleading the tribunal, adjourn for examination and appoint its own expert.[61] The credible challenge procedure proposed in Part III operates entirely within those powers. Its principal virtue is that it brings the question of fabrication forward to the stage at which it can be examined at least cost-effectively and with least damage to finality.

B. After judgment

Where fabrication comes to light after judgment, the routes depend upon timing and forum. An appeal may be brought on the ground that the judgment rested upon unreliable evidence, and the appellate rules permit further evidence to be received in defined circumstances.[62] Ghanaian courts have long held that fraud vitiates a judgment procured by it, so that a judgment obtained on

[56] Advisory Committee on Evidence Rules (n 23); New York City Bar Association, 'Comments on Proposed Federal Rule of Evidence 707 and Amendments to Rule 609' (February 2026) <https://www.nycbar.org/reports/comments-on-proposed-federal-rule-of-evidence-707-and-amendments-to-rule-609/> accessed 30 October 2026.

[57] NRCD 323, s 52 and the provisions on expert opinion.

[58] *State v Loomis* 2016 WI 68, 881 NW 2d 749.

[59] Linda J Skitka, Kathleen L Mosier and Mark Burdick, 'Does Automation Bias Decision-Making?' (1999) 51 International Journal of Human-Computer Studies 991.

[60] Djokoto, 'From Data Protection to Algorithmic Accountability' (n 3).

[61] NRCD 323, ss 6(1) and 52, and the provisions on court-appointed experts.

[62] Court of Appeal Rules 1997 (CI 19), provision on the reception of further evidence.

fabricated evidence may be set aside in fresh proceedings upon proof of the fraud.[63] In the Supreme Court, the review jurisdiction is available in exceptional circumstances where a miscarriage of justice has occurred, including on the discovery of new and important matter that could not, with due diligence, have been produced at the hearing.[64] Each route is real. Each, however, places on the aggrieved person the burden of proving the fabrication to the standard appropriate to disturbing a final judgment, and none supplies the forensic means of doing so.

C. Consequences for the fabricator

The Criminal Offences Act, 1960 (Act 29) criminalizes perjury and the fabrication of evidence, and the deliberate tender of a synthetic record as genuine in judicial proceedings falls squarely within the latter.[65] A legal practitioner who knowingly tenders fabricated evidence is liable to professional discipline.[66] These consequences deter, but they do not restore the person against whom the fabrication was used.

D. The institutional gap

Two deficiencies remain. The first is the absence of any structured mechanism through which a person who believes that a conviction rested upon fabricated digital evidence may obtain independent forensic review once the ordinary appellate process is exhausted. Jurisdictions that have confronted miscarriages of justice at scale have relied upon an independent body with powers to investigate and to refer cases to the appellate courts and, in the exceptional case of Horizon, upon legislation quashing convictions directly.[67] Ghana has no equivalent body. The second is the absence of a statutory scheme of compensation for persons wrongly convicted on fabricated evidence, a gap that the constitutional provision on compensation for unlawful detention does not fully close.[68] Both proposals would require legislation. They are identified here because correction that depends upon a victim's private capacity to prove a sophisticated fabrication will in practice be unavailable to most of those who most need it.

IX. CONFIRMED REQUIREMENTS, ANNOUNCED MEASURES AND PROPOSED SAFEGUARDS

The argument of this article draws upon three categories of norms that must not be confused: requirements confirmed in enacted law, measures announced or published in draft that do not yet bind, and safeguards proposed here for judicial or legislative adoption. Of the twenty matters on which the argument relies, seven are confirmed, five are announced, and eight are proposed. Table 1 records each, so that no proposal or bill is mistaken for the law.

Table 1. Status of the norms relied upon, as at 30 October 2026.

Matter	Position	Principal source	Status
Fair *hearing*; adequate facilities; examination of witnesses	Binding on all courts and organs of state	Constitution, arts 12, 19	Confirmed
Authentication threshold	Evidence sufficient to support a finding that the item is what it is claimed to be	NRCD 323, s 136	Confirmed
Electronic records and the weight factors	No exclusion merely for electronic form; generation, storage, integrity and originator go to weight	Act 772, ss 6, 7	Confirmed
Security duties of public custodians of personal data	Government departments are data controllers bound by the security principle	Act 843, ss 17, 91	Confirmed
Critical information infrastructure; licensing of service providers	In force; directive issued by the Cyber Security Authority	Act 1038	Confirmed (designation of court systems unknown)
Electronic service of process	In force in the High Court	CI 47, Ord 7 r 3A	Confirmed

[63] *Dzotepe v Hahormene III* [1984-86] 1 GLR 294.

[64] Constitution, art 133; Supreme Court Rules 1996 (CI 16), r 54.

[65] Criminal Offences Act 1960 (Act 29), provisions on perjury and the fabrication of evidence.

[66] LI 2423 (n 43).

[67] Criminal Appeal Act 1995 (UK), pt II; Post Office (Horizon System) Offences Act 2024 (UK).

[68] Constitution, art 14.

Matter	Position	Principal source	Status
Fraud vitiates judgment; perjury and fabrication of evidence are offences	In force	Case law; Act 29	Confirmed
Electronic filing, authentication and service as standard	Announced to commence on 1 October 2026	Chief Justice, 29 July 2026	Announced
Revised Rules of Court	To be laid at the opening of the 2026/27 legal year	Chief Justice, 29 July 2026	Announced
Cybersecurity (Amendment) Bill, 2025	Would confer investigative and data-preservation powers; not enacted	Consultation draft	Announced
Electronic Transactions Bill, 2025	Would repeal Act 772; not enacted	Consultation draft	Announced
Emerging Technologies Bill	Expected in Parliament in 2026; not enacted	Ministerial statements	Announced
Credible challenge procedure	For judicial adoption within NRCD 323	Part III	Proposed
Presumptive court expert where a party cannot fund examination	Requires institutional funding	Part V	Proposed
Inquisitorial provenance questions for unrepresented parties	Within the existing judicial duty	Part V	Proposed
Custodian's account of security measures as bearing on weight	For judicial adoption	Part VI	Proposed
Restricted handling of intimate and fabricated exhibits	For practice direction	Part VI	Proposed
Disclosure conditions for analytical instruments	Condition of reliance on machine opinion	Part VII	Proposed
No ruling on authenticity upon an instrument's output alone	Principle of judicial evaluation	Part VII	Proposed
Post-appeal forensic review and compensation	Requires legislation	Part VIII	Proposed

The distribution is itself revealing. Every announced measure concerns the digitisation of court processes or the regulation of technology at large. None addresses the evidential treatment of synthetic or contested digital records in adjudication, which is the gap the proposed safeguards are designed to fill.

X. THE EVIDENCE REQUIRED TO EVALUATE IMPLEMENTATION

None of the requirements or safeguards discussed above can be assessed without information that is not at present published. The first task for the Judiciary, regulators and researchers is therefore to make the evidential system itself observable. The evaluative questions fall into three groups: what happens in courtrooms when digital exhibits are contested; whether the custodians of digital records, the Judiciary included, maintain the conditions of integrity on which weight depends; and whether correction is available when fabrication is discovered. Table 2 identifies, for each question, the evidence that would answer it, the body most likely to hold that evidence, and the route by which it might be obtained.

Table 2. Evidence required to evaluate implementation.

Evaluative question	Evidence required	Likely holder	Route of access
How often are digital exhibits challenged as fabricated, and how are challenges resolved?	Sample of rulings recording challenges, their foundations and outcomes	Judicial Service; law reports; GhaLII	Case-file research with judicial permission; published judgments
Are challenges particularized or bare?	Coding of the stated grounds of challenge in the same sample	Judicial Service	Case-file research

Evaluative question	Evidence required	Likely holder	Route of access
How long does forensic examination take, and who commissions it?	Turnaround times and commissioning party for forensic reports	Investigative agencies	Research agreement; Right to Information Act request
Can unrepresented parties contest digital exhibits?	Challenge rates and outcomes by representation status	Judicial Service case data	Anonymized data release; court observation
Are court experts appointed in digital evidence disputes?	Number of appointments and their funding	Judicial Service	Registry records
How are filed exhibits protected against alteration under E-Justice Plus?	Hashing, access control and audit log specifications; incident records	Judicial Service	Disclosure in litigation; parliamentary question; Right to Information Act request
Are court systems designated as critical information infrastructure?	Designation instrument and attaching obligations	Cyber Security Authority	Authority publication; Right to Information Act request
Are analytical instruments validated, and are error rates disclosed in proceedings?	Validation reports; versions in use; disclosure in sampled cases	Investigative agencies; parties	Disclosure orders; research agreements
Are judges trained on synthetic evidence?	Curricula, attendance and evaluation	Judicial Training Institute	Institutional request; annual reports
Is correction invoked when fabrication is discovered?	Set-aside actions for fraud, review applications and fabrication prosecutions involving digital records	Courts; Attorney-General	Court records; prosecution statistics

Two methodological cautions apply. First, the absence of recorded challenges does not establish the absence of the problem. The American survey in which fifteen of 931 judges reported deepfake challenges measured challenges raised, not fabrications tendered, and an undetected fabrication leaves no trace in a survey of judges.[69] Research in Ghana should therefore combine analysis of the record with forensic re-examination of a sample of admitted exhibits, where consent and law permit. Second, indicators serve accountability only if they are published. A modest set of them, namely challenge rates, forensic turnaround times, court expert appointments, and the security specifications of court systems, could appropriately be reported in the Judicial Service's annual reports.

XI. CONCLUSION

Ghana does not need a statute that names deepfakes before it can begin to protect the integrity of adjudication. What it needs is for its courts to exercise the powers they already have over the evidential burden, disclosure and expert assistance, and for the custodians of digital records, the Judiciary foremost among them, to treat the integrity of the systems they maintain as a condition of proof rather than a matter of administrative convenience.

The argument may be gathered into four propositions. First, the authentication rule in section 136 of the Evidence Act and the weight-based scheme of section 7 of Act 772 remain sound in principle, but they rest upon two premises, the reliability of recognition and the availability of testing, which synthetic media have weakened together. Second, the resulting injustice is in essence a failure of procedural fairness under article 19, because the capacity to test a digital record is unequally distributed. Its correction lies in a credible challenge procedure that moves the evidential burden upon a particularized showing, a presumptive role for court-appointed experts, an inquisitorial supplement for unrepresented parties, and an insistence upon reasoned rulings. Third, the integrity of adjudication now depends upon conditions of custody that precede and surround the trial. The security duties imposed by data protection and cybersecurity law are properly treated as evidential guarantees, and machine assessments of authenticity may inform judicial evaluation but must never displace it. Fourth, the routes by which a judgment resting upon fabrication may be corrected presuppose that the aggrieved person can prove the fabrication, and the absence of an independent post-appeal review mechanism leaves the most vulnerable without effective recourse.

[69] Federal Judicial Center survey (n 24).

The distinction maintained throughout between what the law confirms, what has been announced and what is proposed is a substantive one. Ghana is in the middle of a rapid transition: electronic filing and authentication are becoming standard, revised Rules of Court are pending, and several bills on digital governance are in preparation. In such a period, an announcement is easily mistaken for a safeguard and a draft for a right. The best protection against that error is the discipline that the law of evidence itself demands, which is to ask what can be shown, by whom and upon what record. Applied to the institutions of justice, that discipline yields the evaluative inquiry set out in Part X.

The courts of Ghana have adapted before to changes in the way facts reach them, from the written instrument to the photocopy to the electronic message. The present change differs because it unsettles the court's confidence in its own perception and, through the digitization of court processes, reaches into the court's own record. An adequate response must therefore be both doctrinal and institutional. A court whose rules are sound but whose systems are opaque, or whose systems are secure but whose procedures leave the poorer party unable to test the evidence against it, will not deliver judgments that deserve the public confidence on which its authority ultimately rests.

REFERENCES

1) Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, 1785.
2) Mirjan R Damaška, Evidence Law Adrift (Yale University Press 1997).
3) Godwin E K Djokoto, 'Governing the Public-Sector Acquisition of Artificial Intelligence in Ghana: Data Sovereignty, Human Accountability and the Limits of Technical Oversight' (2026, forthcoming); Godwin E K Djokoto, 'From Data Protection to Algorithmic Accountability: Rethinking Legal Remedies for AI-Assisted Decisions in Ghana' (2026, forthcoming).
4) Godwin E K Djokoto, 'Judicial Standards for Electronic Evidence in Ghana: Building a Coherent Jurisprudence for the Digital Age' (2026, forthcoming); Godwin E K Djokoto, The Manufactured Fact: Truth, Authenticity and Legal Proof in Ghana's Synthetic Information Age (forthcoming).
5) Constitution of the Republic of Ghana 1992, art 19(1), (2)(e), (2)(g) and (13).
6) ibid art 18(2).
7) ibid arts 12(1) and 125(1), (3) and (4).
8) Evidence Act 1975 (NRCD 323), s 136.
9) ibid ss 137 to 142.
10) ibid ss 10 to 17, 51 and 52.
11) Electronic Transactions Act 2008 (Act 772), ss 6 and 7(1).
12) ibid s 7(2).
13) Electronic Transactions Bill 2025 (consultation draft); LEX Africa, 'E-Signed, Sealed and Delivered: Ghana's Current Legal Framework and Proposed Reforms for E-Signatures' (July 2026) <https://lexafrica.com/2026/07/ghanas-current-legal-framework-and-proposed-reforms-for-e-signatures/> accessed 30 October 2026.
14) High Court (Civil Procedure) Rules 2004 (CI 47), Ord 7 r 3A, inserted by the High Court (Civil Procedure) (Amendment) Rules 2019 (CI 122).
15) Ghana News Agency, 'Judiciary to Roll Out Electronic Court Processes from October: CJ' (29 July 2026) <https://gna.org.gh/2026/07/judiciary-to-roll-out-electronic-court-processes-from-october-cj/> accessed 30 October 2026.
16) Data Protection Act 2012 (Act 843), ss 17 and 91; Cybersecurity Act 2020 (Act 1038).
17) Kofi Anokye Owusu-Darko, 'The Data Protection Bill 2025: A Stronger Shield' Business & Financial Times (Accra, 20 May 2026) <https://thebftonline.com/2026/05/20/the-data-protection-bill-2025-a-stronger-shield-what-is-it-meant-to-enable/> accessed 30 October 2026; Cyber Security Authority, 'Public Consultation on the Draft Cybersecurity (Amendment) Bill, 2025' <https://csa.gov.gh/public_document.php> accessed 30 October 2026; 'Gov't to Lay Emerging Technologies Bill before Parliament in 2026' Citi Newsroom (Accra, 5 November 2025) <https://www.citinewsroom.com/2025/11/govt-to-lay-emerging-technologies-bill-before-parliament-in-2026/> accessed 30 October 2026.
18) 'The Rise of AI Deepfake Fraud in Ghana: Inside the Accra High Court Case' Modern Ghana (17 June 2026) <https://www.modernghana.com/blogs/1503245/the-rise-of-ai-deepfake-fraud-in-ghana-inside.html> accessed 30 October 2026.
19) NRCD 323, s 136.
20) Federal Rules of Evidence (US), rr 104(b) and 901(a), and the Advisory Committee Note to r 901.
21) Djokoto, 'Judicial Standards for Electronic Evidence in Ghana' (n 4).
22) NRCD 323, ss 139 to 142.

23) Advisory Committee on Evidence Rules, Agenda Book (May 2026) pt IV <https://www.uscourts.gov/sites/default/files/document/advisory_committee_on_evidence_rules_may_2026.pdf> accessed 30 October 2026.
24) Federal Judicial Center survey (March 2026), reported in 'AI Deepfakes Put Courtroom Evidence Under Growing Cloud of Doubt' Court Cast (16 October 2026) <https://courtscast.com/ai-deepfakes-put-courtroom-evidence-under-growing-cloud-of-doubt-openai-and-meta-warn/> accessed 30 October 2026.
25) Bates v Post Office Ltd (No 6: Horizon Issues) [2019] EWHC 3408 (QB); Hamilton v Post Office Ltd [2021] EWCA Crim 577; Ministry of Justice, Use of Evidence Generated by Software in Criminal Proceedings: Call for Evidence (21 January 2025).
26) Evidence Act 1893 (Singapore), s 116A; Gil v Public Prosecutor [2025] SGCA 21; Bharatiya Sakshya Adhiniyam 2023 (India), s 63.
27) NRCD 323, ss 1 to 4 and 10 to 17.
28) Djokoto, The Manufactured Fact (n 4).
29) Chesney and Citron (n 1); Rebecca A Delfino, 'Deepfakes on Trial: A Call to Expand the Trial Judge's Gatekeeping Role to Protect Legal Proceedings from Technological Fakery' (2023) 74 Hastings Law Journal 293.
30) Kwasi Wiredu, 'Truth as Opinion' in Kwasi Wiredu, Philosophy and an African Culture (Cambridge University Press 1980).
31) Chesney and Citron (n 1) 1785 to 1786.
32) Riana Pfefferkorn, '"Deepfakes" in the Courtroom' (2020) 29 Boston University Public Interest Law Journal 245.
33) Coalition for Content Provenance and Authenticity, C2PA Technical Specification <https://c2pa.org/specifications/> accessed 30 October 2026.
34) Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, arts 50(2), 50(4) and 113.
35) Africa Policy and Development Institute, 'Emerging Technologies Bill' <https://apdigh.org/bills/2-emerging-technologies-bill/> accessed 30 October 2026; 'Ghana's AI and Deepfake Rules: What the New Data Protection Bill Means' Wansom (22 October 2026) <https://www.wansom.ai/briefly/news/ghana-s-ai-and-deepfake-rules-what-the-new-data-protection-bill-means-2026-10-22> accessed 30 October 2026.
36) Act 1038, provision on the non-consensual sharing of intimate images.
37) Djokoto, The Manufactured Fact (n 4).
38) Constitution, art 19(2)(e) and (g).
39) Republic v Eugene Baffoe-Bonnie and Four Others (Supreme Court); Practice Direction (Disclosures and Case Management in Criminal Proceedings) 2018.
40) CI 47, Ord 21.
41) Dombo Beheer BV v Netherlands (1994) 18 EHRR 213, para 33.
42) NRCD 323, provisions on court-appointed experts; Legal Aid Commission Act 2018 (Act 977).
43) Legal Profession (Professional Conduct and Etiquette) Rules 2020 (LI 2423).
44) Djokoto, 'Judicial Standards for Electronic Evidence in Ghana' (n 4).
45) Djokoto, 'Governing the Public-Sector Acquisition of Artificial Intelligence in Ghana' (n 3).
46) Act 843, ss 17, 28 and 91.
47) Act 772, s 6.
48) Data Protection Commission, 'Compliance' <https://dpc.gov.gh/compliance/> accessed 30 October 2026; Data Protection Commission, Guidelines to Demonstrate Data Protection Compliance (2025).
49) Act 1038, provisions on critical information infrastructure; Cyber Security Authority, Critical Information Infrastructure Directive, Risk Assessment Framework and National Cybersecurity Policy and Strategy <https://www.csa.gov.gh/resources.php> accessed 30 October 2026.
50) Bates (n 25); Hamilton (n 25).
51) Act 1038 (n 36).
52) Act 1038, provisions on the licensing of cybersecurity service providers and the accreditation of cybersecurity professionals.
53) Cyber Security Authority (n 17); 'Rethinking the Cybersecurity Amendment Bill' Business & Financial Times (Accra, 25 November 2025) <https://thebftonline.com/2025/11/25/rethinking-the-cybersecurity-amendment-bill/> accessed 30 October 2026.
54) Djokoto, 'From Data Protection to Algorithmic Accountability' (n 3).
55) Laurence H Tribe, 'Trial by Mathematics: Precision and Ritual in the Legal Process' (1971) 84 Harvard Law Review 1329.

56) Advisory Committee on Evidence Rules (n 23); New York City Bar Association, 'Comments on Proposed Federal Rule of Evidence 707 and Amendments to Rule 609' (February 2026) <https://www.nycbar.org/reports/comments-on-proposed-federal-rule-of-evidence-707-and-amendments-to-rule-609/> accessed 30 October 2026.
57) NRCD 323, s 52 and the provisions on expert opinion.
58) State v Loomis 2016 WI 68, 881 NW 2d 749.
59) Linda J Skitka, Kathleen L Mosier and Mark Burdick, 'Does Automation Bias Decision-Making?' (1999) 51 International Journal of Human-Computer Studies 991.
60) Djokoto, 'From Data Protection to Algorithmic Accountability' (n 3).
61) NRCD 323, ss 6(1) and 52, and the provisions on court-appointed experts.
62) Court of Appeal Rules 1997 (CI 19), provision on the reception of further evidence.
63) Dzotepe v Hahormene III [1984-86] 1 GLR 294.
64) Constitution, art 133; Supreme Court Rules 1996 (CI 16), r 54.
65) Criminal Offences Act 1960 (Act 29), provisions on perjury and the fabrication of evidence.
66) LI 2423 (n 43).
67) Criminal Appeal Act 1995 (UK), pt II; Post Office (Horizon System) Offences Act 2024 (UK).
68) Constitution, art 14.
69) Federal Judicial Center survey (n 24).