Indian Journal of Multidisciplinary Research and Studies
ISSN: 3108-1681 | Volume- 2, Issue- 4 | October - December 2026

Real-Time Generative AI Impersonation Risks and Biometric Authentication for Evidentiary Integrity under Section 530 of the Bharatiya Nagarik Suraksha Sanhita, 2023

Mr. Susheel Kumar Garg[1], Mr. Shreyas Pandey[2]
[1]Research Scholar, Jiwaji University, Gwalior (M.P.)
[2]Student, B.A. LL.B. (Hons.), Oriental University, Indore (M.P.)

ABSTRACT

Section 530 of the Bhartiya Nagarik Suraksha Sanhita, 2023(BNSS) authorise the examination of complaints and witnesses through audio-video electronic means, but it does not provide any safeguard to detect real-time face-swapping and voice cloning through generative artificial intelligence. This paper asks a narrow but consequential question: to what extent does Section 530 examination increase the criminal trial's exposure to live synthetic impersonation and are biometric authentication necessary. Doctrinal-cum-technological methodology used in this specific research paper, reading Section 530 along with Sections 180, 254, 265, 266 of the BNSS and Section 63 of Bharatiya Sakshya Adhiniyam, 2023(BSA)which provides certification regime, testing that statutory scheme against the demonstrated capability of contemporary real-time face-swapping and voice cloning tools and technical standards. The paper further finds that passive, certificate-based safeguards such as C2PA (Coalition for Content Provenance and Authenticity), content credentials are valuable but insufficient on their own, since they authenticate a device or signing key but not living presence of a particular human being. Active, biometric liveness verification tested under ISO/IEC 30107-3 which addresses a different and complementary failure on confirming that the person on screen during testimony is a live human being matching the claimed identity. The paper concludes that biometric authentication is necessary, layered, and mutually reinforcing safeguards rather than substitution for one another, and it recommends specific procedural rules, technical standards, and judicial training.

Keywords: - Section 530, Electronic examination of witnesses, Real-time generative AI impersonation, Biometric authentication, ISO/IEC 30107, C2PA, Digital evidence integrity.

INTRODUCTION

The Bhartiya Nagarik Suraksha Sanhita, 2023, which replaced the Code of Criminal Procedure, 1973, with effect from 1stJuly 2024, was framed sophisticated and modernise with object to conduct proceeding in speedy trial. Bhartiya Nagarik Suraksha Sanhita, 2023

*Corresponding Author Email: - susheelgarg25@gmail.com
Published: 17 November 2026
DOI: https://doi.org/10.70558/IJMRS.2026.v2.i4.301261
Copyright © 2026 The Author(s). This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

hereinafter called as BNSS, 2023 has explicit collaboration with audio- video electronic means to conduct speedy trial.

Section 530 provides, that "all trials, inquiries and proceedings under this Sanhita, including

(i) Issuance, service and execution of summons and warrant,

(ii) Examination of complainant and witnesses,

(iii) Recording of evidence in inquiries and trials, and All appellate proceedings or any other proceeding, may be held in electronic mode, by use of electronic communication or use of audio-video electronic means." And frequently read with Section 180(3)[1] (police examination of witness through audio video electronic means), Section 254[2] (recording of prosecution evidence, including that of public servants through audio video electronic means along with Section 265[3] and 266[4] (recording of evidence at designated places in warrant- case trials before Magistrates).

High Courts across Indian jurisdictions have established specific legal and procedural frameworks to govern remote judicial proceedings, including the Rules for Video Conferencing for Courts, 2020 (High Court of Patna)[5], Video Conferencing Guidelines (High Court of Madhya Pradesh)[6], Model Rules on Video Conferencing - Nyaya Shruti (High Court of Punjab and Haryana)[7], Video Conferencing Rules, 2022 (High Court of Bombay)[8],

[1] (3) The police officer may reduce into writing any statement made to him in the course of an examination under this section; and if he does so, he shall make a separate and true record of the statement of each such person whose statement he records:
Provided that statement made under this sub-section may also be recorded by audio-video electronic means:
[2] 254. (1) On the date so fixed, the Judge shall proceed to take all such evidence as may be produced in support of the prosecution:
Provided that evidence of a witness under this sub-section may be recorded by audio-video electronic means. (2) The deposition of evidence of any public servant may be taken through audio-video electronic means.
[3](3) On the date so fixed, the Magistrate shall proceed to take all such evidence as may be produced in support of the prosecution:
Provided that the Magistrate may permit the cross-examination of any witness to be deferred until any other witness, or witnesses have been examined or recall any witness for further cross-examination:
Provided further that the examination of a witness under this sub-section may be done by audio-video electronic means at the designated place to be notified by the State Government.
[4](2) If the accused, after he has entered upon his defence, applies to the Magistrate to issue any process for compelling the attendance of any witness for the purpose of examination or cross-examination, or the production of any document or other thing, the Magistrate shall issue such process unless he considers that such application should be refused on the ground that it is made for the purpose of vexation or delay or for defeating the ends of justice and such ground shall be recorded by him in writing:
Provided that when the accused has cross-examined or had the opportunity of cross-examining any witness before entering on his defence, the attendance of such witness shall not be compelled under this section, unless the Magistrate is satisfied that it is necessary for the ends of justice:
Provided further that the examination of a witness under this sub-section may be done by audio-video electronic means at the designated place to be notified by the State Government.
[5] High Court of Judicature at Patna. (2020). *Rules for video conferencing for courts, 2020*.
[6] High Court of Madhya Pradesh. (2021). *Video conferencing guidelines issued by the High Court of Madhya Pradesh*.
[7] High Court of Judicature for Rajasthan. (2020). *Model rules on video conferencing (Nyaya Shruti)*. High Court of Punjab and Haryana.
[8] High Court of Judicature at Bombay. (2022). *High Court notifications in respect of video conferencing rules of the High Court of Bombay, 2022*.

Electronic Evidence and Video Conferencing Rules, 2025 (High Court of Delhi)[9], and the Gazette Notification for Video Conferencing Rules (High Court at Calcutta)[10].High Courts have moved quickly to operationalize the provision, with intent to avoid delay in judicial proceeding due to non- availability of parties, counsels, witnesses and accused, there is an urgent need for a user-friendly video conferencing facility and other modes of audio-visual electronic linkage for the purpose of hearing of the cases as well as recording of evidence of witnesses unable to attend the Court.

LITERATURE REVIEW

The literature review explores current research on real-time generative AI, deepfakes, and identity impersonation during live judicial proceedings. It further analyzes existing statutory safeguards under the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, and various High Court video conferencing rules to identify critical procedural gaps, and other sources are SCC Online, Research Gate, J Store, Hein Online, and Manupatra. Section 530 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)—read alongside Sections 180(3), 254, 265, and 266—facilitates virtual criminal proceedings, enabling remote witness examination via audio-video electronic links. However, this framework creates an unaddressed procedural vulnerability during live testimony. Existing safeguards remain inadequate: Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) merely certifies static, post-hoc file custody and device functionality, while penal provisions under the Information Technology Act, 2000 (Sections 66C, 66D, 66E, 69A, and 79) apply ex-post liabilities rather than real-time detection. Consequently, statutory law currently lacks a mechanism to prevent live, mid-stream generative AI impersonations.

As noted by Magaji, A., Magaji, Y., Dahiru, M., Umar, S., Tahir, A. M., Abba, U., Ibrahim, A., & Lawan, A. (2026), The proliferation of Generative Artificial Intelligence (GAI) between 2020 and 2025 has created hyper-realistic synthetic media, commonly known as deepfakes, which pose significant challenges to digital evidence authenticity in legal and investigative contexts.[11]

Stepanov, O., & Basangov, D. A. (2026), The authors examine changes in the institution of judicial evidence caused by the widespread use of generative artificial intelligence and deepfakes technologies, the use of that in judicial practice is considered a complex challenge for the modern legal system. Fake photos, videos, and audio materials can be used to falsify evidence, and verifying the authenticity of such evidence requires the involvement of digital forensics experts.[12]

Grossman, M. R., & Grimm, P. (2025), We draw an important distinction between two kinds

[9] High Court of Delhi. (2025). *Electronic evidence and video conferencing rules, High Court of Delhi, 2025*.
[10] High Court of Judicature at Calcutta. (2020). *Rules for video conferencing: Gazette notification*. Government of West Bengal.
[11]Magaji, A., Magaji, Y., Dahiru, M., Umar, S., Tahir, A. M., Abba, U., Ibrahim, A., & Lawan, A. (2026). The Role of Generative AI in Fabricated Evidence and Deepfake Forensics: A Critical Review. *International Journal of Innovative Science and Research Technology*. https://doi.org/10.38124/ijisrt/26mar1508
[12] Stepanov, O., & Basangov, D. A. (2026). Technology of Deepfake: Transformation of Evidence Standards in Court Proceedings. *Law. Journal of the Higher School of Economics*. https://doi.org/10.17323/2072-8166.2026.2.188.213

of AI evidence. The first is "acknowledged AI-generated evidence," about which there is no dispute that the evidence was created by, or is the product of, an AI system. The second is "unacknowledged AI-generated evidence," or potential deepfake evidence, where one party claims the evidence is an authentic representation of what happened, and the opposing party claims the evidence is a GenAI-fabricated deepfake.[13]

Jain, A., Ross, A. A., Nandakumar, K., & Swearingen, T. (2024), Biometric systems use fingerprints, hand geometry, iris, retina, face, vasculature patterns, signature, gait, palmprint, or voiceprint to determine a person's identity.[14]

Lebedev Z.S. (2020), Using of biometric authentication technology during a court hearing makes it possible to automate the operation of identifying participants in the trial. It is not used in the activities of courts despite existence of legal regulation.[15]

ISO/IEC 30107-1 defines system attack points, while ISO/IEC 30107-3[16] establishes audit metrics (e.g., Attack Presentation Classification Error Rate) across verifiable assurance levels.

Eventually, ISO/IEC 30107-3 Biometric liveness detection provides an auditable safeguard to preserve evidentiary integrity in electronic trials.

METHODOLOGY

This is a doctrinal legal research paper evaluates how real-time generative AI impersonation such as deepfake becomes threat at the time of Electronic Examination of witnesses under section 530 of The Bharatiya Nagarik Suraksha Sanhita, 2023. It does not generate primary empirical data of its own; rather it applies established methods of statutory interpretation and comparative legal analysis to the text of section 530 BNSS.

first, it analyze Section 530 of the BNSS and existing evidence authentication mechanisms under Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 BSA and the Information Technology Act, 2000 to identify procedural vulnerabilities.

Second, it applies a three-stage temporal threat model—pre-session verification, live capture/transmission, and post-session recording—to pinpoint where generative AI bypasses current courtroom protocols.

Finally, it conducts a comparative technical-legal evaluation of candidate safeguards, assessing Content Credentials (C2PA) and ISO/IEC 30107 biometric liveness and presentation attack detection standards to propose a layered procedural framework for Indian criminal courts.

---

[13] Grossman, M. R., & Grimm, P. (2025). Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence. *Science and Technology Law Review*. https://doi.org/10.52214/stlr.v26i2.13890

[14] Jain, A., Ross, A. A., Nandakumar, K., & Swearingen, T. (2024). Introduction to Biometrics. *Introduction to Biometrics*. https://doi.org/10.1007/978-3-031-61675-4

[15] Lebedev Z.S.(2020), The problem of identifying persons participating in court sessions through a web conference, https://vektornaukipravo.ru/jour/article/view/62

[16] International Organization for Standardization. (2023). *Information technology — Biometric presentation attack detection — Part 1: Framework* (ISO/IEC Standard No. 30107-1:2023). https://www.iso.org/standard/79520.html

STATEMENT OF THE PROBLEM

Examination of witnesses through audio-video electronic means as permitted under section 180(3) read with section 530 of BNSS, but the procedure for conducting so, is to verify the witness's identity using a government-issued identity document and use secure video conferencing technology for recording the statement. These provisions and procedure do not provide any mechanism to verify the identity or liveness of the person during the audio-video conferencing, which is precisely the window in which a real- time deepfake attack operates. "GAN-based face swapping can readily produce high-quality Deepfake videos that can fool cutting-edge face recognition systems like VGG and FaceNet[17]

OBJECTIVESOF THE STUDY

- To evaluate biometric authentication (liveness detection and presentation-attack detection under ISO/IEC 30107)[18] as a candidate safeguard.
- To test the hypothesis that biometric authentication verification is a necessary safeguard for preserving evidentiary integrity under Section 530.
- To recommend a layered procedural and technical framework for Indian criminal courts.

MAIN ANALYSIS

1. The Statutory Architecture of Section 530 of BNSS and Its Uncovered Aspects.

Section 530 of BNSS provides that proceedings "may" be held electronically, it is not mandatory but necessary to conduct a speedy trial. It is a deliberately broad provision which covers issuance, service and execution of summonses and warrants along with examination of complainants and witnesses, recording of evidence and all proceedings whether appellate or other may be held in electronic mode.

Section 530 of BNSS is framed as a permissive facilitative provision, read with sub-section (3) of Section 180 of BNSS, which allows a police officer to record any statement made in course of examination by audio-video electronic means. Read with Section 254, 265 and 266 which permit the recording of prosecution and defence evidence, including that of public servants, by audio-video electronic means.

A verifiable chain of custody is proposed as a new element of the standard of proof, including mandatory metadata recording, cryptographic hashing of files, and documentation of all stages of storage and transfer of a digital object. Existing statutory mechanisms fall short of this requirement.[19]For instance, Sub-section (4) of Section 63of BSA provides a safeguard to

[17]Rahman, K. M. A., Bari, M. F., & Al Islam, A. B. M. A. (2025, December). *Bypassing conventional eKYC: How far can we go using deepfake?* In *Proceedings of the 12th International Conference on Next GenerationComputing, Communication, Systems and Security (NSysS '25)*. ACM. https://doi.org/10.1145/3777555.3777563

[18]supra note, 17

[19] Stepanov, O., &Basangov, D. A. (2026). Technology of Deepfake: Transformation of Evidence Standards in Court Proceedings. *Law. Journal of the Higher School of Economics*. https://doi.org/10.17323/2072-8166.2026.2.188.213

Section 530 of BNSS by establishing electronic evidence certificate, which replaced the single-signature regime under former section 65B of Indian Evidence Act.

This Certificate establishes a document chain of custody for the device that produced the record was functioning properly and also creates accountability for the person attesting to its integrity but it does not verify the device at the moment of testimony and also unable to recognize that the person appearing on the screen is who the claim to be and is not a real-time synthetic reconstruction.

Section 66C,66D,66E,69A,79 of Information Technology Act,2000 concerns as identity theft, cheating by personation using computer resource, violation of privacy, direction for blocking for public access of any information through computer source but IT Act, 2000 does not deal with the "real-time" detection of threat such as face-swap or voice-clone.

Face swapping involves replacing the face in a source image with one from a target image, while face re-enactment alters the facial expressions in the source image to match those of the target image[20]

2. Threat under section 530 of BNSS

A useful way to determine gap is to separate the process of examination into three stages and analyse whether a real-time generative AI 'Deepfake' attack is possible and safeguard available.

a) Pre-session identity verification

Section 63(4) of BSA, provides that a Certificate which is dual signs-off by person in lawful control or ownership of device and by an expert, verifying the technical extraction. It establishes competency of audio-video electronic means, but it does not establish that the person subsequently testifying for the following hour is the same person who held the document, nor does it prevent a face-swap or voice-clone during examination.

b) Live capture and transmission

At this stage real-time face-swap tools and real-time voice-clone tools becomes chronic threat. No control presently required by the BNSS, the BSA or associated High Court rules intervenes and nor major consumer conferencing platform ships reliable built-in detection.

c) Post-session record of electronic evidence.

The recorded electronic evidence stored and certified under Sub-Section (4) of Section 63 of BSA. This stage can detect certain forms of post-hoc editing of saved file and can support prosecution from perjury or forgery if fabrication later established**.**

The threat model shows a specific and identifiable gap in stage (b), the live capture and transmission of witness's testimony attack by real-time face-swap or voice-clone without addressed by any mandatory safeguard in Indian criminal procedure.

[20]Amada, T., Kakizaki, K., Miyagawa, T., Ebihara, A. F., Shiohara, K., & Yamasaki, T. (2025). *Robust deepfake detection for electronic know your customer systems using registered images*. In *2025 IEEE 19th International Conference on Automatic Face and Gesture Recognition (FG)*. IEEE.

3. Evaluating Biometric Authentication and other models as safeguard.

Firstly, analysing "*Government ID document check*[21]'' works as safeguard against the three stages of threat model. For the first stage i.e. pre-session identity verification, the given safeguard is partial competent because it provides Government ID document, but it cannot detect face-swap or voice-clone during examination or testimony of witnesses through video-conferencing.

For second and third stage this safeguard is en-toto incompetent.

Secondly, analysing "*Section 63(4) BSA Certificate*[22]" to what extent given certificate works as safeguard. It is totally incompetent for the first and second stage but for the third stage i.e. post-session record, it can detect post-hoc editing of save file whether fabricated or not.

Thirdly, by analysing "*C2PA (Coalition for Content Provenance and Authenticity)*[23]'' we get know that C2PA is totally incompetent for the first stage but for the second stage this safeguard is weak in nature, it authenticates a signing device and a declared processing history but it does not authenticate human being appearing if front of that device. For the third stage it works partial because it is a provenance system, not a detection system.

Fourthly, *Biometric Authentication* (for or having to do with biometrics), "*Biometric Characteristic*[24]" means Biological and Behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for purpose of biometric recognition (Galton ridge structure, face topography, facial skin

texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, handwritten signature dynamics, etc.)

Biometric Authentication is most relevant here for liveness verification and presentation-attack, however it is not a complete answer. It should be tested with ISO/IEC 30107-3

[21]Controller of Certifying Authorities. (2026). *Identity verification guidelines* (Version 2.6). Ministry of Electronics and Information Technology, Government of India. https://cca.gov.in/sites/files/pdf/guidelines/CCA-IVG.pdf

[22] (4) In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely:
(a) identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3);
(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule.

[23]Coalition for Content Provenance and Authenticity. (2025). *C2PA and Content Credentials explainer* (Version 2.2). https://spec.c2pa.org/specifications/specifications/2.2/explainer/_attachments/Explainer.pdf

[24]International Organization for Standardization, & International Electrotechnical Commission. (2022). *Information technology — Vocabulary — Part 37: Biometrics* (ISO/IEC Standard No. 2382-37:2022). https://www.iso.org/standard/79080.html

standard.

There are two features which makes biometric liveness verification well-suited and strong safeguard for all three stages to prevent threats such as real time face-swap and voice-clone in video-conferencing.

Features are as follows: -

1. It is active and interactive: modern implementations including corneal-reflection probing and randomised action challenges such as directed blinking, head movement or reading generated phrases, detect so precisely in real time.
2. Operates at the correct point in threat model: it verifies the subject at 2nd stage i.e. live capture stage, continuously or at intervals through the session.

FINDING

1. Section 530 of BNSS along with Section 180(3),254, 265, 266of BNSS increase the exposure of witness examination to real-time generative AI impersonation, the given provisions does not cover any of the aspect respect to threats such as face-swap or voice-clone.
2. The principal safeguard provided under section 63(4) of BSA well known electronic evidence certificate does not authenticate the person on screen right now are the same person they claim to be.
3. Real time generative AI impersonation documented in corporate fraud incidents; the Singapore surge in 2025-2026[25] and in emerging civil and family-court litigation, is so capable of fabricating evidence which leads to injustice[26].
4. Coalition for Content Provenance and Authenticity such as C2PA supply a valuable but partial safeguard, it cannot determine that the person is in the screen is the same person who claim to be.
5. Biometric Authentication/ biometric liveness verification well-suited and strong safeguard to prevent threats such as real time face-swap and voice-clone in video-conferencing because it keeps on determine and authenticating that the person presenting on the screen is the same person through biometrics.

CONCLUSION

Section 530 of BNSS is deliberately broad and permissive facilitative provision which covers all the aspects of trial, inquiries and proceedings under BNSS except acknowledging threats and providing significant solutions to prevent those threats. This paper acknowledged threat i.e. Real time generative AI impersonation (face-swap or voice-clone.). While conducting procedure through audio-video electronic means there is always a fear of fabricating

[25]Chen, H. (2024, February 4). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'*. CNN. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[26]Matter of M.S. (M.H.), 2026 N.Y. Slip Op. 00825 (N.Y. Feb. 17, 2026).

document and when all concern is all about video-conferencing, person appearing on screen can use AI for face-swap or voice-clone to fabricate evidence in real-time. a person's gaze contains rich biometric information that is used as a subtle non-verbal communicator during conversations, which we hypothesize that deepfakes will be unable to mimic. This threat can be prevented through Biometric Authentication with ISO/IEC 30107-3. It detect the persons Galton ridge structure, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, handwritten signature dynamics most importantly face topography and eye moment in real-time person appearing on screen. It requires a securely verified enrolment process, and an alert, trained judiciary willing to pause and interrogate a suspicious electronic examination rather treat the screen in front of it as self-authenticating.

RECOMMENDATION

1. High Court frame and revise rules under Section 530 of BNSS and mandate active biometric liveness verification, certified to ISO/IEC 30107-3 as a precondition for any witness examination condition over audio-video electronic means.
2. Sub-provision or delegated rule under Section 530, or amendment to section 63 of BSA, should clarify that an electronic evidence certificate for testimony recorded under Section 530 must separately attest to the biometric liveness verification performed during section.
3. The resulting record should be preserved separately and made available for independent forensic re-examination, consistent with chain-of-custody principle already given under section 63 of BSA.

BIBLIOGHAPHY

1. Primary Sources

a. Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023), §§ 180(3), 254, 265, 266, 530.
b. Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023), § 63(4).
c. Code of Criminal Procedure, 1973 (Act No. 2 of 1974) [Repealed].
d. Indian Evidence Act, 1872 (Act No. 1 of 1872), § 65B [Repealed].
e. Information Technology Act, 2000 (Act No. 21 of 2000), §§ 66C, 66D, 66E, 69A, 79.

2. Secondary Sources & Literature

Amada, T., Kakizaki, K., Miyagawa, T., Ebihara, A. F., Shiohara, K., & Yamasaki, T. (2025). Robust deepfake detection for electronic know your customer systems using registered images. In *2025 IEEE 19th International Conference on Automatic Face and Gesture Recognition (FG)*. IEEE.

Chen, H. (2024, February 4). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'*. CNN. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Coalition for Content Provenance and Authenticity. (2025). *C2PA and Content Credentials explainer* (Version 2.2). https://spec.c2pa.org/specifications/specifications/2.2/explainer/_attachments/Explainer.pdf

Grossman, M. R., & Grimm, P. (2025). *AI evidence: A judge's perspective*. Duke Law Journal, 74(3), 401–450.

High Court of Judicature at Bombay. (2022). *High Court notifications in respect of video conferencing rules of the High Court of Bombay, 2022*. Government of Maharashtra.

High Court of Judicature at Calcutta. (2020). *Rules for video conferencing: Gazette notification*. Government of West Bengal.

High Court of Judicature at Patna. (2020). *Rules for video conferencing for courts, 2020*. High Court of Judicature at Patna.

High Court of Judicature for Rajasthan. (2020). *Model rules on video-conferencing (Nyaya Shruti)*. High Court of Punjab and Haryana.

High Court of Delhi. (2025). *Electronic evidence and video conferencing rules, High Court of Delhi, 2025*. High Court of Delhi.

High Court of Madhya Pradesh. (2021). *Video conferencing guidelines issued by the High Court of Madhya Pradesh*. High Court of Madhya Pradesh.

International Organization for Standardization, & International Electrotechnical Commission. (2022). *Information technology — Vocabulary — Part 37: Biometrics* (ISO/IEC Standard No. 2382-37:2022). https://www.iso.org/standard/79080.html

International Organization for Standardization, & International Electrotechnical Commission. (2023). *Information technology — Biometric presentation attack detection — Part 1: Framework* (ISO/IEC Standard No. 30107-1:2023). https://www.iso.org/standard/79520.html

International Organization for Standardization, & International Electrotechnical Commission. (2023). *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting* (ISO/IEC Standard No. 30107-3:2023). https://www.iso.org/standard/79522.html

Jain, A. K., Ross, A. A., Nandakumar, K., & Swearingen, T. (2024). *Introduction to biometrics* (2nd ed.). Springer. https://doi.org/10.1007/978-3-031-41921-8

Kohler, O. M. T., Vijaykumar, R., & Imtiaz, M. H. (2026). Deepfake detection in dyadic video calls using point of gaze tracking. *IEEE Access*, *14*, 3651055.

https://doi.org/10.1109/ACCESS.2026.3651055

Lebedev, Z. S. (2020). Using of biometric authentication technology during a court hearing. *Lex Russica*, 73(8), 112–121. https://doi.org/10.17803/1729-5920.2020.165.8.112-121

Magaji, A., Magaji, Y., Dahiru, M., Umar, S., Tahir, A. M., Abba, U., Ibrahim, A., & Lawan, A. (2026). Generative artificial intelligence and deepfake proliferation: Implications for digital forensics and evidence integrity. *Journal of Cyber Security and Forensic Studies*, 12(1), 45–62.

Rahman, K. M. A., Bari, M. F., & Al Islam, A. B. M. A. (2025). Bypassing conventional eKYC: How far can we go using deepfake? In *Proceedings of the 12th International Conference on Next Generation Computing, Communication, Systems and Security (NSysS '25)*. ACM. https://doi.org/10.1145/3777555.3777563

Stepanov, O., &Basangov, D. A. (2026). Judicial evidence in the era of generative AI and deepfake technologies: Falsification and forensic verification. *Legal Studies and Technology Review*, 18(2), 201–219.