



DIGITAL DECEPTION: AI AND THE LAW OF EVIDENCE

By *Aishwarya Pandit*

From *Thakur Ramnarayan College of Law*

By *Vaishnavi Shetty*

From *Thakur Ramnarayan College of Law*

ABSTRACT

The Indian courtroom has undergone significant transformation over the years. Earlier, cases largely relied on handwritten letters, physical documents, and oral testimonies given by witnesses in person. Today, a large number of cases depend substantially on digital evidence such as smartphone data, WhatsApp conversations, call logs, CCTV recordings, emails, and digitally signed contracts. In many situations, such electronic records are no longer merely supplementary but form the very foundation of the case. With the enactment of the Information Technology Act, 2000, Section 65B was introduced into the Indian Evidence Act, 1872 to establish a structured mechanism for the admissibility of electronic records through a certification process confirming their creation and storage. The Bharatiya Sakshya Adhiniyam, 2023, which came into force on 1 July 2024, has largely retained this framework while introducing certain additional provisions of its own. But due to rapid growth of generative artificial intelligence, creation of deepfake images, cloned voice recordings, fabricated WhatsApp chats, and digitally manipulated documents that can appear entirely authentic. The paper delves into this pertinent issue, it examines the statutory definition and taxonomy of evidence under the Bhartiya Sakshya Adhiniyam, 2023, and traces the doctrinal evolution of electronic evidence in India. It interrogates whether the existing certification under Section 63 and related provisions adequately addresses AI-generated manipulation. The paper further analyses the

evidentiary risks posed by synthetic media and evaluates the sufficiency of current admissibility standards, burdens of proof, and forensic safeguards. The central issue addressed in this paper is whether the existing legal framework governing electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 is adequately equipped to deal with the rise of AI-generated digital content

Keywords :*Evidence, electronic, digital, artificial intelligence, AI*

INTRODUCTION

The term 'evidence' is derived from the Latin word 'evidens' or 'evidere', which means "to show clearly; to make clear to the sight; to discover clearly; to make plainly certain; to ascertain; to prove"¹ In the legal sense, evidence refers to the means by which facts in issue are proved or disproved before a court of law. The law of evidence is an adjective law to procedural laws; it is the very medium through which those rights are validated or exonerated. The Bharatiya Sakshya Adhiniyam, 2023 (hereinafter referred to as 'BSA') is the principal statute governing the law of evidence in India for proceedings initiated on or after July 1, 2023. It replaced the Indian Evidence Act, 1872 hereinafter referred as ('IEA') a statute that had governed Indian evidence law for over 150 years. The BSA was enacted as part of a comprehensive legislative reform package that also included the Bharatiya Nyaya Sanhita, 2023² and the Bharatiya Nagarik Suraksha Sanhita, 2023³.

Under the BSA Section 2(1)(e)⁴ "evidence" means and includes (i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence; (ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence; this definition forms the foundation of the

¹ RATANLAL & DHIRAJLAL, THE LAW OF EVIDENCE 3 (Justice Arijit Pasayat ed., 27th ed. 2020).

² replacing the Indian Penal Code, 1860.

³ replacing the Code of Criminal Procedure, 1973.

⁴ Bharatiya Sakshya Adhiniyam, 2023



entire evidentiary framework. The definition is inclusive, not exhaustive, the word ‘includes’ shows that they are illustrations of a broader concept, not an exhaustive list. The evidence is bifurcated into two categories: oral evidence (statements made by witnesses) and documentary evidence (documents produced for the court’s inspection). For the purposes of this paper, the definition explicitly states that documentary evidence includes electronic or digital records. Electronic and digital records are documentary evidence in the fullest and most unqualified sense under the BSA. The IEA’s definition of ‘evidence’ did not, as originally enacted in 1872, mention electronic records; they were brought within the definition through the definition of ‘document’ (Section 3 IEA) and through the specific provisions of Sections 65A and 65B. The BSA, by contrast, places electronic and digital records squarely within the core definition of evidence from the outset.

The evidence is mainly classified into oral evidence, as defined in Section 2(1)(e)(i) of the BSA, it consists of all statement given including electronic which court requires to be made before it, in relation to matter of fact. The BSA, following the IEA, requires oral evidence to be direct.⁵ Section 39 of the BSA, expressly recognises the admissibility of statements recorded through audio-visual electronic means, including video conferencing, a recognition that became urgent during the COVID-19 pandemic and has since become institutionalised in Indian courts.

The Supreme Court’s Model Rules for Video Conferencing for Courts, 2020, remain operational under the BSA framework. On the other hand, documentary evidence consists of documents produced for the court’s inspection. Under the IEA, a document was defined to mean any matter expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.⁶ The IT Act, 2000

amended this definition to include electronic records. It is further classified, for purposes of proof, into primary evidence and secondary evidence. Under the BSA, section 56 defines primary evidence as the document itself produced for the court’s inspection. Section 57 talks about what are different kinds of primary evidence, in contrast to previous provision under section 62 of the IEA, in S.57 under explanation 4 to 7, expressly recognise various forms of electronic and digital records such as multiple files created during storage, records produced from proper custody, stored video recordings, and automated storage across computer resources as constituting primary evidence. While it does extend the scope of application, it mainly focuses on the manner in which electronic records are stored or produced before the court. As a result, a digital image, video, or audio file may qualify as primary evidence merely by virtue of being produced in its original electronic form. In relation to synthetic media, such as deepfakes, this classification could potentially allow manipulated or AI-generated material to be admitted into evidence without undergoing adequate technical or forensic scrutiny at the stage of admissibility. Section 58 defines secondary evidence as including certified copies, copies made by mechanical processes, copies made from the original by other means, counterparts, and oral accounts of the contents of the document. For electronic records specifically, the Supreme Court in *Anvar P.V. v. P.K. Basheer*,⁷ clarified that the computer or device on which the electronic record is stored constitutes, in a sense, the original but that it is the output (print-out, CD, screenshot) that is produced before the court as secondary evidence.

EVOLUTION OF ELECTRONIC EVIDENCE IN INDIA

Electronic record under the Indian Evidence act is first mentioned in Section 2(d) where of Indian evidence where while defining the term ‘document’, in its illustration at “(vi) *An electronic record on emails, server logs, documents on computers, laptop or*

⁵ Section 57 of the Bharatiya Sakshya Adhiniyan, 2023

⁶ Section 3 of the Indian Evidence Act,

⁷ (2014) 10 SCC 473



smartphone, messages, websites, locational evidence and voice mail messages stored on digital devices are documents.” This qualifies and include any sort of document which when can be printed through and can be available. Before the emergence of the IT act the term, electronic evidence was not widely referred anywhere, prior to this majority of cases with respect to electronic evidence were those of tape recordings, etc. In *State of Maharashtra v. Prakash Vishnu Rao Mane*,⁸ the Bombay High Court examined the admissibility of tape-recorded evidence and treated it as a form of mechanical or electronic recording. Further, while laying down practical guidelines, the Court suggested taking assistance of electronic experts and referred to the growing use of tape-records and the electronics, emphasizing the need for proper legislative regulation.

The Information Technology Act, 2000 was enacted primarily to give legal recognition to e-commerce and digital transactions, the IT Act had profound implications for the law of evidence. It amended the Indian Evidence Act, 1872, By amending the Indian Evidence Act, 1872, the Banker’s Books Evidence Act, 1891, and the Indian Penal Code, 1860. The IT Act introduced the following key amendments to the IEA that govern electronic evidence:

- a) Section 65A was inserted that clarified that electronic records were to be provided in the strict manner prescribed under Section 65B.
- b) Section 65B further provided that any information contained in an electronic record, when printed, stored, recorded, or copied onto optical or magnetic media by a computer, is deemed to be a document. Such electronic output is admissible as evidence of the contents of the original electronic record without requiring production of the original, provided the conditions set out in sub-section (2) are satisfied and a certificate as required under sub-section (4) is furnished.

- c) Sections 85A and 85B introduced statutory presumptions in respect of electronic records and digital signatures. Section 85A creates a presumption regarding the authenticity of electronic contracts executed using a digital signature. Section 85B, in civil proceedings, raises a presumption that a secure electronic record has remained unaltered since the point in time to which the security relates, unless proved otherwise.
- d) Section 88A: This provision creates a presumption that an electronic message forwarded by the originator through electronic means was indeed sent by the purported originator. The burden is thereby shifted to the opposing party to disprove or rebut the authenticity of the communication.

The first major judicial conflict with Section 65B arose in *State (NCT of Delhi) v. Navjot Sandhu*.⁹ the case was concerning the Indian Parliament attack of 2001, call detail records between the people who were accused of the said crime were used as evidence. These records were adduced without a 65b the certificate. The accused then argued that the records should not be admitted or relied in evidence because, the State had not complied with 65b certification.. A two-judge bench of the Supreme Court observed, “*Irrespective of the compliance of the requirements of Section 65B which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely Sections 63 & 65. It may be that the certificate containing the details in sub-Section (4) of Section 65B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely Sections 63 & 65.*” As two witnesses were examined from the telecom companies, who produced printouts of the call details and during cross-examination, no serious challenge was raised regarding tampering or fabrication. The

⁸ 1977 79 BOMLR 217

⁹ (2005) 11 SCC 600



Court held that under Sections 63 and 65, secondary evidence is admissible where the original cannot be easily produced, and since the call data was stored in large servers that could not be physically brought to court, certified printouts taken by mechanical process and proved through competent witnesses could be admitted as secondary evidence.¹⁰ The Court thus ruled that non-compliance with Section 65B did not automatically bar admissibility if secondary evidence was otherwise permissible, effectively allowing electronic records such as call data to be admitted even without a Section 65B certificate. This observation though it can be characterised as obiter created lasting confusion. For nearly a decade, courts across India in *Kundan Singh vs. State*,¹¹ *Avadut Waman Kushe vs The State of Maharashtra*,¹² admitted electronic evidence without Section 65B certificates, relying on oral expert testimony instead. The Navjot Sandhu approach effectively made the certificate optional, which Parliament had never intended.

The decision of Navjot Sandhu was overruled by a 3-judge bench of Supreme Court in *Anvar P.V. v. P.K. Basheer & Ors.*,¹³. This was an election petition, the dispute arose as CDs and a pen drive containing audio-visual recordings of alleged electoral offences, were tendered in evidence without a Section 65B certificate. The Court held that Sections 63A and 65B of the Evidence Act constitute a special and complete code for proving electronic records. Since Section 65B is a special provision specifically enacted to deal with electronic evidence, it overrides the general provisions relating to secondary evidence under Sections 62 and 63 of the Evidence Act. Applying the legal maxims that is 'genelis special non derogant,' that special law prevails over general law, the Court held that the mode of proof prescribed under Section 65B is mandatory and exclusive. The CDs and pen drives in the case, were excluded from evidence.. This case established three propositions of cardinal importance, first, that Section 65B is a complete and

exclusive code for the admission of secondary electronic evidence; second, that the certificate under Section 65B (4) is a condition precedent to admissibility; and third, that oral evidence of the contents of an electronic record without a certificate is inadmissible.

This was followed by another landmark judgement of *Tomaso Bruno v. State of Uttar Pradesh*,¹⁴ where two Italian nationals were found guilty of murdering a fellow tourist in Agra. While determining the admissibility of CCTV footage, the court observed as CCTV comes under the category of electronic record, it must be proved in conformity of Section 65B provision. The original DVR (Digital Video Recorder) was seized and produced before the trial court, bringing it closer to primary evidence territory. The Court held that when the original recording device is produced before the court, the certificate requirement under Section 65B is not mandatory, it only becomes essential when secondary copies are produced.¹⁵. Further 2-bench judge in *Shafi Mohammad v. State of Himachal Pradesh*,¹⁶ introduced a relaxation of the certificate requirement that directly conflicted with Anvar. The Court observed that, practical difficulties may arise for accused persons or complainants who do not have control over the devices from which the electronic records are produced. The Court reasoned that to insist on a certificate in such cases would deny them access to evidence that might be vital to their case. This resulted in a clear and irreconcilable conflict between the two-judge bench decision in Shafi Mohammad and the earlier three-judge bench ruling in Anvar. The divergence in views also led to considerable uncertainty at the trial court level, with different courts adopting different approaches regarding the requirement and timing of the Section 65B certificate.

This judicial inconsistency was ultimately settled by a 5-judge Constitutional bench decision in *Arjun Panditrao Khotkar v. Kailash Kushanrao*

¹⁰ Id. ¶ 65.

¹¹ 2015 SCC OnLine Del 13647

¹² 2016 SCC OnLine Bom 3236

¹³ (2014) 10 SCC 473

¹⁴ (2015) 7 SCC 178

¹⁵ Id. ¶ 25.

¹⁶ (2018) 2 SCC 801



Gorantya.¹⁷ The case arose from yet another election petition, where video recordings without Section 65B certificates had been admitted. The Constitution Bench held as follows:

'The certificate required under Section 65B (4) is a condition precedent to the admissibility of evidence by way of electronic record. Failure to produce the said certificate renders such evidence inadmissible... Secondary evidence of the contents of a document must always be distinguished from proof of an electronic record under Section 65B. Secondary evidence of the contents of an electronic record is governed by Section 65B alone.'

Additionally, the Constitution Bench held that an objection to the admissibility of electronic evidence for want of a certificate must be raised at the time of admission; objections at the appellate stage will not be entertained unless the court is satisfied that it was not reasonably possible to raise the objection earlier.

The Bharatiya Sakshya Adhiniyam which replaced the Indian evidence act, expressly includes 'electronic' or digital records within the definition of documentary evidence.¹⁸ It incorporates the said reference from the definition of electronic record u/s 2(1)(t) of the IT Act, 2000. It encompasses any form of data that is stored, received, or sent in electronic form regardless of the technology used, the medium of storage, or the nature of the content. With respect to other provisions related to the evidence are replicated similarly in the new act, Section 61 of BSA corresponds to Section 65B, it retains the certification necessary for secondary electronic evidence and the four conditions for admissibility are retained verbatim. Notably, the BSA does not introduce any new mechanism with respect to any AI generated images, videos etc.

PRINCIPLES GOVERNING AUTHENTICITY OF ELECTRONIC EVIDENCE.

As discussed above the primary mechanism for admissibility of any electronic record, is that either the device be produced directly in the court for it to be

considered primary evidence, and if such is not possible in case of emails, WhatsApp chat etc., their printout/transcribes if produced be tendered with the a 63B certificate, to conclusive established the authenticity of the said document. The process of authentication involves establishing that the evidence is what it claims to be. In case of electronic evidence, authentication assumes a vital role, it means to demonstrate that the electronic record was created or sent by the person alleged to have created or sent it, that it has not been altered since creation or transmission, and that it accurately represents the event or communication it purports to document. Throughout the whole process, the certificate is compulsory and it only establishes the chain of custody of the evidence from the original device to the output produced before the court. The scope of the said certificate is limited to the following:

- i. the identity of the computer or electronic device from which the output was generated
- ii. that the device was used regularly during the relevant period for the stated activities
- iii. that information of the kind in the electronic record was regularly fed into the device in the ordinary course of those activities
- iv. that the device was operating properly during the relevant period
- v. that the output reproduces the information as it was stored in the device.

The foundational jurisprudence for such technical scrutiny can be traced to *Ram Singh v. Col. Ram Singh*,¹⁹ where the Supreme Court of India laid down safeguards for the admissibility of tape-recorded evidence. The Court held that recordings are admissible only if the speaker's voice is properly identified, the accuracy of the recording is proved, the possibility of tampering or erasure is ruled out, the content is relevant, and the recording is kept in proper custody. Recognising that magnetic recordings are

¹⁷ (2020) 7 SCC 1

¹⁸ 2(1)(e) of the Bharatiya Sakshya Adhiniyam, 2023.

¹⁹ AIR 1986 SC 3



susceptible to manipulation, the Court insisted that such evidence must be received with caution and subjected to rigorous verification, almost akin to scientific proof. Apart from this, in terms of forensic examination, in some cases, if requested, from this a digital forensic expert examining an electronic record also analyses metadata such as timestamps, device identifiers, server logs, and application version history. The expert may also conduct hash verification, a cryptographic hash (e.g., MD5 or SHA-256) generates a unique digital fingerprint of a file; if the hash value at the time of production matches the value generated at the time of extraction, it strongly indicates that the file has not been altered.²⁰ Such examination also assists in verifying chain of custody and detecting deletion, insertion, or modification. The above principles are limited in their scope and applicability; they restrict themselves to the chain of custody of the device. The 65B certificate is a process certificate, not a content certificate. It limits itself to the chain of custody, not the authenticity of the content. In the vast majority of cases involving WhatsApp chats, emails, or other digital communications, parties rely solely on a Section 65B certificate to secure admissibility. Once the certificate is produced, the court ordinarily admits the electronic record without insisting on any deeper technical scrutiny. Forensic examination enters the picture only when the authenticity of the said evidence is disputed or when the circumstances suggest possible manipulation. Even then, its role in Indian litigation remains crucial but insufficiently formalised. Under Section 45 of the Bharatiya Sakshya Adhiniyam, 2023, courts may seek expert opinion on matters involving science or technical knowledge. Although the section does not mention about any particular type of experts, traditionally, the courts have relied only on experts in the fields of forensic, medical, handwriting etc. However, the said section is silent with regards to

experts on artificial intelligence systems and algorithmic outputs. With the rapid advancement of Artificial Intelligence, such type of evidence is more than likely to appear in court. A traditional digital forensic expert may not possess the skills to differentiate and understand the specialized machine-learning expertise required to detect algorithmic manipulation. As the statute does not recognize such experts, it again poses a burden on the court to determine the appropriate qualifications, expertise, and credibility of such experts. Consequently, judges may be required to independently assess whether a proposed expert possesses sufficient technical competence to assist the court, which may create inconsistencies in the admission and evaluation of expert testimony. It thus becomes imperative that the statute, or any supplementary procedural rules, establish clear standards for the recognition and qualification of experts in areas such as artificial intelligence and digital forensics. The formal recognition of specialized AI forensic experts would assist courts in assessing the authenticity and reliability of technologically complex evidence and would strengthen the overall evidentiary framework governing electronic records.

ARTIFICIAL INTELLIGENCE IN THE EVIDENTIARY FRAMEWORK

The term 'artificial intelligence' is the most commonly used yet the least clearly understood term in today's public discourse. Its meaning has evolved a lot since it was first coined by John McCarthy and Marvin Minsky at the Dartmouth Summer Research Project in 1955, where they described it as an idea where every aspect of human intelligence, such as reasoning, learning, and even problem-solving, could in theory be described so deeply and precisely that a machine could be programmed to imitate it.²¹ The primary goal of building a machine that thinks in the same ways as

²⁰ Kent, K. et al. (2006) Guide to integrating forensic techniques into incident response, CSRC. Available at: <https://csrc.nist.gov/pubs/sp/800/86/final> (Accessed: 03 March 2026).

²¹ McCarthy, J. et al. (no date) A proposal for the Dartmouth Summer Research Project on Artificial

Intelligence, August 31, 1955, AI Magazine. Available at: <https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904> (Accessed: 05 March 2026).



a human has never been achieved, yet it has never been abandoned either; the only thing that has changed is the way the researchers have tried to make the above goal a reality. At its most basic level, artificial intelligence refers to a set of computer tasks that, if performed by humans, would require a certain level of intelligence. It covers various sets of abilities.

For instance, a spam filter that can detect unwanted emails, a navigation app that can change your path in real time, a chess program that can defeat a world chess champion, and a generative system that can draft legal documents in the span of seconds or create a set of believable WhatsApp messages. All these are different outcomes of artificial intelligence. The Association for the Advancement of Artificial Intelligence defines AI as the scientific study of the processes behind thought and intelligent behaviour and how these can be built into machines. In 2020, the European Parliament explained AI in simpler terms as a machine having the ability to show human-like skills such as explaining, creating, reasoning, and problem-solving.²² The evolution of artificial intelligence as a research domain has experienced what researchers frequently refer to as the ‘hype cycle’. There are stages of significant expectations and public enthusiasm, succeeded by disillusionment when major advancements do not occur as swiftly as anticipated.

This is followed by a more subdued phase where genuine technical advancements take place, typically without much fanfare, and then the enthusiasm begins to escalate once more. Since it began in the 1950s, the field has gone through at least two full cycles like this. Many believe we are now at the peak of a third and especially intense phase. What makes this wave different is not just the massive private and government funding, partly influenced by strategic competition between the United States and China, which some compare to the Cold War space race, but

also the fact that certain abilities, especially in generative AI, have finally reached a level that earlier periods only talked about in theory.

To really understand the power of modern AI and the threat it poses to the authenticity of all electronic evidence, it’s important to understand, at least in a broad manner, how AI systems are actually made. The foundation of most significant and extraordinary innovations in the last few decades is based on artificial neural networks, which are at their core inspired by the structure of a human brain. A neural network contains layers and layers of interconnected processing nodes, all of which take numerical imprints and then perform mathematical operations and pass the results forward to the next layer. The connections between nodes carry numerical weights that determine the strength of their influence. When the network is trained, it is exposed to very large quantities of labelled data, such as images paired with descriptions, text paired with translations, and audio paired with transcripts, and the weights of the connections are iteratively adjusted to minimize the difference between the network’s output and the correct answer.²³ ‘Deep learning’ refers specifically to neural networks of many successive layers, sometimes numbering in the hundreds. The depth of these networks enables them to learn representations of increasing abstraction: early layers detect simple patterns such as edges and colours; intermediate layers combine these into shapes, textures, and local structures; later layers recognize complex, high-level features such as faces, spoken words, or the stylistic patterns of a particular writer. It is this capacity for hierarchical, multi-level pattern recognition that distinguishes deep learning from earlier AI approaches and that accounts for the dramatic improvements in performance across domains that have occurred since approximately 2012.²⁴ The training of these models requires enormous

²² Association for the Advancement of Artificial Intelligence, “Welcome to AAAI” <<https://www.aaai.org>> accessed 26 February 2026.

²³ Rumelhart, D.E., Hinton, G.E. and Williams, R.J. Learning representations by back-propagating errors,

Nature News. Available at: <https://www.nature.com/articles/323533a0> (Accessed: 01 March 2026).

²⁴ Krizhevsky, A., Sutskever, I. and Hinton, G.E. (2012) Imagenet classification with deep



computational resources, such as specialized processors running for weeks or months on datasets of billions of examples. Once trained, however, applying the model what engineers call ‘inference’ is computationally cheap, which is why these capabilities can be delivered to millions of users simultaneously through ordinary web browsers and smartphone applications.

A. Generative AI: The Revolution in Content Creation

The AI systems of greatest relevance to the law of evidence are not those that classify or analyze existing content but those that create new content. Generative AI is the category of artificial intelligence that produces original text, images, audio, and video from a given prompt or specification. Three technological developments have driven the generative AI revolution and are directly implicated in the fabrication of electronic evidence: large language models, diffusion models for image and video synthesis, and AI-powered voice cloning. Large language models such as GPT-4, Claude, Llama, and Gemini undergo training involving hundreds of billions of words gathered from various sources, including the internet, books, and other written materials. In the course of this training, they absorb the statistical patterns of language across all dimensions: grammar, vocabulary, tone, style, factual information, and even the unique characteristics of specific authors.²⁵ When given a specific prompt, these AI systems generate texts or paragraphs aligned with the patterns they have thoroughly learned. This ability allows them to form coherent sentences, human-sounding dialogues, and organized content, including made-up conversations that have never

particularly occurred. If a model receives examples of someone’s WhatsApp messages or emails, it can produce new messages “in their style,” closely imitating their word choices, sentence structures, frequent phrases, and personal expressions. For an average reader and often even for a judge, there may be no clear indication that the interaction was generated artificially.²⁶ Voice cloning technology, accessible via commercial services like Eleven Labs and several open-source applications, is capable of creating synthetic speech that replicates an individual’s voice with just three to five seconds of actual audio. The system analyzes the distinctive sound characteristics of that voice, including pitch, tone, rhythm, and speaking style, and subsequently produces new speech from any written text that aligns closely with those attributes. In numerous instances, the outcome sounds so authentic that even experienced listeners can struggle to identify the difference. This presents a significant evidentiary hazard. A forged audio recording of an individual supposedly confessing to a crime, making a threat, or acknowledging a debt can be created without that person ever voicing those statements. The file can then be stored on a device and subsequently presented in court with a technically accurate certificate under Section 65B, despite the fact that the content itself is completely false.

B. Deepfakes

Deepfakes are manipulations of video content to a place; a person’s face as well as voice are digitally inserted into situations, they were never actually a part of. When this particular technology became accessible around 2017, early deepfakes could be very easily spotted because the faces were not particularly visible;

convolutional neural networks. advances in neural information processing systems, 25, 1097-1105. Available at: <https://www.scirp.org/reference/referencespapers?referenceid=3031254> (Accessed: 04 March 2026).

²⁵ Brown, T. et al. (1970) Language models are few-shot learners, *Advances in Neural Information Processing Systems*. Available at:

<https://papers.nips.cc/paper/2020/hash/1457c0d6bfc4967418bfb8ac142f64a-Abstract.html> (Accessed: 05 March 2026).

²⁶ Ai Deception: A survey of examples, risks, and potential solutions. Available at: <https://arxiv.org/pdf/2308.14752> (Accessed: 04 March 2026).



they were blurred slightly around the edges in some videos, the people blinked weirdly, and the lip movements never properly matched the audio. But the technology has drastically improved since then. Modern deepfakes have surpassed the "uncanny valley" effects by employing Generative Adversarial Networks (GANs) and diffusion models that analyze extensive hours of video to perfect skin textures and lighting. Current AI doesn't merely superimpose a face; it replicates how light interacts with a person's skin and how their neck muscles exert tension during speech, rendering the junction between the artificial face and the real body undetectable. Beyond visual accuracy, the availability of these technologies has shifted from being available solely to expert academics to anyone who possesses a smartphone.

The genuine difficulty that generative AI presents to the justice system transcends technicalities; it is fundamentally structural. The resources required to produce fraudulent electronic evidence, such as a counterfeit WhatsApp chat, a replicated voice recording, or a deepfake video, are available for free, readily accessible, and user-friendly. An individual equipped with merely a smartphone and an internet connection can generate highly realistic false evidence in just a matter of minutes. Conversely, the instruments needed to identify such fabrication are expensive, require specialized forensic knowledge, and typically yield results that are probabilistic rather than definitive. Their precision also hinges on the advancement of the generative model and the sophistication of the fabricated output. As generative technology advances, current detection systems become less dependable, necessitating the creation of new detection techniques, which are subsequently anticipated and evaded by the following generation of generative tools.

In the recent years, India has witnessed a sharp and visible rise in litigation concerning AI-generated misuse of celebrity identity. Recently celebrities such

as. Amitabh Bachchan,²⁷ Anil Kapoor,²⁸ have approached the Delhi High Court, in particular, for urgent interim injunctions against deepfakes, AI voice cloning, and digital impersonation. In several of these cases, the courts have prohibited such as unauthorized advertisements or merchandise, AI-generated replicas, including synthetic voiceovers, manipulated interviews, and fabricated endorsements circulating across social media platforms. In other cases, the Bombay HC in Arijit Singh v. Codible Ventures LLP,²⁹ where it directly confronted the misuse of generative AI. The case involved unauthorized AI-generated songs and voice clones that simulated the singer's voice and persona. The Court expressed serious concern over the vulnerability of celebrities to misuse through unauthorized generative AI content. It observed that the defendants were exploiting the plaintiff's popularity to attract traffic to their platforms by enabling the creation of counterfeit audio and video content using the plaintiff's name, voice, image, and persona without consent. Such unauthorized use, particularly for commercial purposes, was considered capable of causing significant economic harm to the plaintiff's career and reputation.³⁰

Another issue which comes from AI is its use by law professionals as well as judiciary for drafting and pleadings and case citing. There have been cases where fake case names were added in the said pleading. Other nation in the world also is facing similar issue, the UK High Court rebuked lawyers for citing fake, AI-generated case law in litigation, warning that failure to verify such outputs could constitute contempt or perverting the course of justice. Similarly, the federal district court of USA in Mata v. Avianca, Inc.³¹ sanctioned lawyer for submitting fabricated case citations generated by ChatGPT, emphasizing that AI-derived misinformation in legal filings can attract penalties and dismissals. Similar concerns have also arisen in India. The Supreme Court, while taking note of the issue, has cautioned

²⁷ 2022 SCC Online Del 4110

²⁸ 2023 SCC OnLine Del 6914

²⁹ 2024 SCC OnLine Bom 2445

³⁰ Id. ¶ 19.

³¹ 678 F. Supp. 3d 443 (2023)



against the reliance on AI-generated and non-existent judicial precedents in pleadings and judicial orders. On 27 February 2026, the Court took cognisance of a situation where a trial court had relied upon non-existent judicial precedents, potentially generated through artificial intelligence tools. The Court observed that reliance on such fabricated authorities does not merely amount to an error in judicial reasoning, but may constitute misconduct affecting the integrity of the adjudicatory process.³²

THE CURRENT LEGAL FRAMEWORK: INDIA & INTERNATIONAL PERSPECTIVES

The international community has not been silent and has always actively addressed the threats posed by technological changes. Instead of remaining passive, they have responded with an impressive number of soft law principles and guidelines aimed at restoring trust in digital evidence. From late 2023 to early 2026, we witnessed the gradual formation of a complex system of global governance. This system begins with wide-ranging, principle-driven frameworks established by the United Nations and progresses towards more detailed regulatory measures such as the strict content-labeling requirements implemented by China, the risk-based transparency mandates developed by the European Union, and ongoing deliberations within the US federal judiciary regarding possible changes in evidentiary duties for cases concerning AI-generated content.

A. The United Nations

The UN has taken a leading role in laying down the normative framework of governance for artificial intelligence. It has been recognized that the issues relating to the fabrication of digital evidence and its capacity are not just technological problems but are

deeply connected to the rule of law as well as the protection of human rights. In March 2024, the United Nations General Assembly adopted Resolution A/78/L.49, titled “Seizing the opportunities of safe, secure, and trustworthy artificial intelligence systems for sustainable development.”³³ This was the first expansive multinational agreement on AI governance, which was co-sponsored by over 120 states.

Fundamentally, the resolution emphasizes that rights afforded to individuals offline should be equally upheld online throughout the entire lifecycle of an AI system. In September 2024, the United Nations strengthened this by adopting the Global Digital Compact (GDC) as an addition to the Pact for the Future. The GDC establishes a more detailed and well-researched framework for digital collaboration, placing significant importance on the integrity of information. This carries a clear note for judicial systems. A vow to maintain a safe and secure digital environment inherently necessitates the establishment of standards concerning traceability, transparency, and interoperability. Digital records must increasingly be accompanied by verifiable metadata and provenance documentation, especially in international contexts where issues of authenticity and admissibility often arise. The UN High-Level Advisory Body on Artificial Intelligence has emphasized that accountability must continue to be firmly human-centered in order to support these endeavors.³⁴ Its guidance states that human actors, especially judges, must maintain clear accountability over AI-assisted procedures in order to protect human rights. This insight is reflected in the already well-recognized “human-in-the-loop” principle. Artificial intelligence (AI) tools can help organize, classify, or semantically parse vast amounts of evidence, but they cannot

³² Gummadi Usha Rani & Anr. Vs. Sure Mallikarjuna Rao & Anr, SLP (C) No. 7575 of 2026, Order dated 27 February 2026 (SC).

³³ General Assembly adopts Landmark Resolution on Artificial Intelligence | UN News (no date) United Nations. Available at: <https://news.un.org/en/story/2024/03/1147831> (Accessed: 05 March 2026).

³⁴ UN Secretary-General’s High Level Advisory Body on Artificial Intelligence, Governing AI for Humanity: Final Report (United Nations, September 2024) (https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf) (Accessed: 04 March, 2026)



replace the subjective intellectual assessment that forms the basis of fact-finding. Judicial decision-making incorporates moral judgment, interpretation, and reasoning in addition to mechanical processes. In this regard, the UN's new framework clearly positions AI as a tool rather than an arbiter in the administration of justice, without rejecting it.

B. The Council of Europe

The Council of Europe has made significant progress by adopting the first legally binding international convention that expressly addresses the nexus between artificial intelligence, human rights, democracy, and the rule of law. Following the lengthy negotiations between its 46 member states and observer nations like the US, Canada, and Japan, the "Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law" was made available for signature on September 5, 2024.³⁵

The Convention's requirement that governments establish efficient oversight mechanisms and clearly define the acceptable extent of AI deployment is one of its distinguishing characteristics. According to this definition, an AI system is a machine-based system that deduces how to produce outputs that could affect real-world or virtual environments based on the input it gets. In order to keep developing types of AI within regulatory bounds, this functional definition is purposefully broad. The Convention's emphasis on procedural protections and guarantees is crucial for the judicial system. States must make sure that people are provided with proper knowledge when engaging with AI systems and that they are provided with sufficient information to comprehend and contest judgments made by these systems. This upholds the fundamental ideas of natural justice, particularly the

right to be heard and the right to contest evidence. The convention offers helpful guidelines when it comes to AI-generated evidence. "Reliability" is positioned as a principle alongside accountability and openness. There are immediate evidentiary ramifications to this. It permits judicial demand for proper technical scrutiny. If a litigant submits a video that appears to be a deepfake. A court will have justified reasons in requiring information regarding the system that is used, its training data, and safeguards built into the same. By doing this, the Convention ensures that ease of technological freedom does not override personal freedom or compromise the fairness of proceedings. Instead of rejecting AI completely, it conditions its use on demonstrable compliance with rule-of-law standards.

C. Singapore and Australia

Both Singapore and Australia have devised carefully customized procedures in the Asia-Pacific region to ensure that AI tools do not compromise the human authenticity of legal evidence. The 2025 Guide for Using Generative AI in the Legal Sector issued by Singapore's Ministry of Law emphasizes three core principles: transparency, confidentiality, and professional ethics. It makes clear that while AI can assist legal work, it does not diminish a lawyer's professional responsibilities. This position is further supported by Singapore's earlier Guide on the Use of Generative AI Tools by Court Users. Instead of focusing only on data protection or technological norms, these governments have actively addressed how generative AI may impact the integrity of witness testimony.³⁶ The guide expressly forbids the creation, embellishment, strengthening, or dilution of evidence using generative AI. Advocates may take help of AI to create an initial draft of an affidavit, but

³⁵ Commission signed the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, democracy and the rule of law Shaping Europe's digital future. Available at: <https://digital-strategy.ec.europa.eu/en/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights> (Accessed: 04 March 2026).

³⁶ Singapore's Digital & AI Governance: A Pro-Innovation, Framework-Driven Model, accessed March 4, 2026, <https://blogs.duanemorris.com/duanemorrisandselva/2026/03/03/singapores-digital-ai-governance-a-pro-innovation-framework-driven-model/>



they are ultimately responsible for the final product. Above all, the witness statements must be accurately represented in the affidavit. The regulation acknowledges that even slight linguistic polishing by AI may unintentionally change tone, certainty, or nuance, which could affect how courts interpret a testimony.

Australia has adopted a far more systematic approach to the regulations. The Federal Court's judges demonstrated institutional concern at the highest judicial level in April 2025 by starting discussion on formal AI usage guidelines. Meanwhile, New South Wales courts established especially stringent practice guidelines.³⁷ Generative AI cannot be used for the creation or alteration of a witness statement in accordance with changes to the Uniform Civil Procedure Rules. Affidavits now must explicitly state that they were prepared without the aid of AI tools. This required certification reflects the assumption that a witness's unvarnished expression is intimately related to the veracity of their statement.

D. China

China has translated AI governance ideas into legally binding technological regulations faster than the majority of other governments. The "Measures for the Labelling of Artificial Intelligence-Generated and Synthetic Content" and the required national standard GB 45438-2025 went into effect on September 1, 2025.³⁸ When combined, these instruments create one of the world's most comprehensive and required AI labeling frameworks, emphasizing traceability and evidentiary accountability in addition to transparency. The Chinese government distinguishes between classifications that are 'implicit' and 'explicit'. Watermarks, symbols, and textual disclaimers are examples of visible signs that let viewers know that the content was created or modified by artificial

intelligence (AI). On the other hand, implicit labels are integrated into the file's metadata. These invisible marks carry information such as the service provider's identity and a unique content identification number. Even if visual markings are eliminated, this dual-layer approach ensures that a technological audit can track the material's history. Additionally, social media companies need to issue notices that are visible to the public in order to maintain implicit tagging. Even if there isn't a label but the content looks to be AI-generated, platforms still need to provide a warning. Private middlemen essentially take on the role of gatekeepers for regulations. India should adopt China's dual layer labelling structure especially the implicit metadata embedding requirement for admissibility of evidence.

India

In the Indian Evidence Act, 1872, the Section 65B, required that any electronic record produced in the form of a computer output must be accompanied by a certificate confirming its authenticity.. The new provision continues the requirement of a certificate for electronic records but expands and modernizes the said framework. In comparison to earlier provision, there was no standard format prescribed, every court interpreted it on their own basis. The BSA on the other hand introduced a standard format, it also made compulsory to include the expert testimony, along with hash value. While this development did strengthen the verification of the integrity of electronic records, it does not fully address the problem of AI-generated or manipulated content. The certificate primarily focuses on the technical process and the chain of custody of the electronic record. It does not require any verification of the actual content of the image, video, or other digital material. The February 2026 amendment to the Information Technology (Intermediary Guidelines and Digital

³⁷ Guide to the protocols and use of AI in Australian Courts - Smokeball, accessed March 4, 2026, <https://www.smokeball.com.au/blog/guide-to-the-court-protocols-on-ai-in-australian-courts>

³⁸ China Releases New Labeling Requirements for AI-Generated Content - Inside Privacy, accessed March

4, 2026, <https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/>



Media Ethics Code) Rules, 2021 marks India's most direct regulatory intervention into AI-generated content so far. Issued by the Ministry of Electronics and Information Technology through G.S.R. 120(E), the amendment moves beyond reactive content moderation and introduces a framework of proactive algorithmic accountability. It formally defines "deepfake" as algorithmically generated audio-visual content that convincingly imitates real persons, while excluding routine edits and accessibility enhancements. Most strikingly, it reduces the takedown timeline from 36 hours to just three hours upon receipt of a valid court order or authorized governmental notice, signalling an urgency-driven compliance model. The amendment further mandates technical disclosure and traceability mechanisms requiring intermediaries to embed metadata or other persistent markers in AI-generated content and imposes operational auditing obligations at periodic intervals. Dispute resolution timelines have also been shortened to seven days. While safe harbour protections remain tied to due diligence, the strengthened language shifts from "endeavour" to mandatory compliance, narrowing discretion.

❖ SUMMARY OF FINDINGS & RECOMMENDATIONS

As discussed above, the current framework governing the admissibility of electronic evidence in India is, at best, procedurally robust but substantively limited. The statutory scheme under the Information Technology Act, 2000 and now under the Bharatiya Sakshya Adhinyam, 2023, has formally integrated electronic and digital records into the definition of documentary evidence and retained the certification requirement under Section 61 (formerly Section 65B). However, the framework is primarily concerned with the manner of production and the functioning of the device, not with the genuineness of the content itself. The certificate authenticates process, not truth. In the age of generative artificial intelligence where fabricated chats, cloned voices, manipulated images, and deepfake videos can be created with alarming ease this limitation becomes critical. A technically compliant certificate can accompany entirely

synthetic material. The existing regime presumes that electronic records, once properly certified, possess a degree of inherent reliability. That presumption no longer holds in the generative AI era. The study further finds that forensic safeguards remain reactive and inconsistently invoked. Although Section 45 of the BSA permits expert opinion and tools such as metadata analysis and hash verification, there is no systematic mechanism requiring content-level authentication where AI fabrication is plausible. This creates a structural imbalance: the production of false digital evidence is cheap, rapid, and accessible, while detection is costly, technical, and often probabilistic. Comparative analysis demonstrates that several jurisdictions are proactively addressing these concerns through transparency mandates, AI-labelling framework, ethical obligations for legal professionals, and institutional safeguards grounded in human accountability. In contrast, India's evidentiary law has not yet evolved to directly confront the risks posed by generative AI within the courtroom itself.

In light of these findings, this paper advances a set of targeted recommendations aimed at bridging the gap between procedural admissibility and substantive reliability.

A. Implement a "Content Authenticity" Requirement Beyond Chain of Custody:

One of the most urgent reforms required in India's evidentiary framework is the adoption of a distinct content- authenticity standard that goes beyond mere proof of chain of custody. As discussed, a video, audio file, or document may be entirely algorithmically fabricated yet remain perfectly preserved from the moment of download or seizure. Accordingly, the said content authenticity certificate must evolve to include mechanisms such as watermark verification, cryptographic signatures, mandatory metadata disclosure, or forensic certification confirming that the material has been examined for synthetic indicators.



B. Possible Amendment to the Bharatiya Sakshya Adhiniyam, 2023:

A possible reform within the BSA would be to create a presumption, that in cases, involving images, videos, WhatsApp chats, or other electronic media, the absence of a recognised authenticity certificate may affect the admissibility of such evidence. In such circumstances, the court may decline to rely upon the electronic record unless the party producing it furnishes the necessary certification establishing its authenticity. The said statutory backing for such a requirement would strengthen the evidentiary framework and place a greater responsibility on parties to ensure the reliability of digital material produced before the court.

C. Establish Specialized Digital Forensic Standards for AI Detection:

It is recommended that the Government of India, through MeitY, mandate the adoption of a C2PA-based Content Credentials framework for specified categories of digital content. This can be introduced by way of an amendment to the Information Technology Act, 2000, along with supporting rules prescribing the technical standards and manner of implementation. The mandate should, at the very least, apply to all digital content generated and published by government ministries, departments, and public authorities, so that such material carries verifiable provenance metadata at the time of creation. Further, officially recorded audio-visual material prepared by public agencies, as well as digitally signed electronic documents, should incorporate such content credentials to ensure traceability and integrity. The compliance with the prescribed C2PA framework may create a rebuttable presumption of authenticity, without making non-compliant material automatically inadmissible. This would strike a balance between strengthening reliability and preserving access to justice.

D. Judicial Training and Forensic Laboratory:

The National Judicial Academy and State should mandate continuing education on AI and Generative technologies, including their technical foundations.

The Central should also equip the Central and State Forensic Laboratory with AI detection technology, supported by licensed software, high spec hardware training.

❖ **CONCLUSION**

Due to its rapid development and global integration Artificial Intelligence has become an important part of our daily life. From automated customer service and predictive analytics to generative tools capable of producing hyper-realistic images, video, and audio. The emergence of artificial intelligence (AI)-generated synthetic media, or “deepfakes,” is one of the most alarming trends. These days, these tools with near accuracy replicate human features, sounds, gestures, and expressions. For the untrained sight, what was formerly clearly identifiable as artificial is now nearly identical to reality. Thanks to technical advancements, people can now produce fake photos or films that seem to show actual people doing things or saying things they never did. The consequences are far reaching and include financial fraud, emotional trauma, political manipulation, and damage to one's reputation. The criminal justice system is particularly vulnerable to such abuse. AI-generated content can be purposefully inserted to deceive law enforcement or judges in a time when electronic evidence is crucial to investigations and prosecutions. It is possible to offer fabricated CCTV footage, morphed images, or recorded confessions as legitimate evidence. If proper forensic verification mechanisms are absent or inadequately implemented, such material may influence investigative direction or judicial reasoning. This creates a serious risk of wrongful arrest, malicious prosecution, and even false conviction. Traditional principles governing admissibility of electronic records were framed in an era where digital manipulation required technical expertise and was comparatively easier to detect. Today, AI tools are widely accessible, inexpensive, and capable of producing content that can bypass superficial scrutiny. In conclusion, while AI is a transformative force with immense potential for societal advancement, its unregulated or inadequately regulated use poses serious threats to individual rights and the integrity of



the justice system. The law must evolve in parallel with technological advancement.

REFERENCES

● **Acts**

1. Indian Evidence Act, 1872
2. The Code of Criminal Procedure, 1973
3. Indian Penal Code, 1860
4. Bharatiya Sakshya Adhinyam, 2023
5. Bharatiya Suraksha Sanhita, 2023
6. Information Technology Act, 2000 (21 of 2000), as amended by the Information Technology (Amendment) Act, 2008
7. Digital Personal Data Protection Act, 2023 (22 of 2023)
8. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
9. EU Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council), Official Journal of the European Union, July 12, 2024
10. Federal Rules of Evidence (US), as amended to December 1, 2023
11. People's Republic of China, Provisions on the Administration of Deep Synthesis Internet Information Services (2023)

● **Case Law**

1. State of Maharashtra v. Prakash Vishnu Rao Mane , 1977 79 BOMLR 217
2. State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru, (2005) 11 SCC 600
3. Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473
4. Tomaso Bruno & Anr. v. State of U.P., (2015) 7 SCC 178 (Supreme Court of India)
5. Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801
6. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1
7. Ram Singh & Ors. v. Col. Ram Singh, 1985 Supp SCC 611

8. Mata v. Avianca Inc., 678 F. Supp. 3d 443 (2023)
9. Kundan Singh v. State, 2015 SCC OnLine Del 13647
10. Avadut Waman Kushe v. The State of Maharashtra, 2016 SCC OnLine Bom 3236

● **Books**

1. Sarkar, S.C., Sarkar on Evidence (17th ed., LexisNexis Butterworths, New Delhi, 2022)
2. Avtar Singh, Principles of the Law of Evidence (26th ed., Central Law Publications, Allahabad, 2021)
3. Mason, Stephen (ed.), Electronic Evidence (4th ed., University of London Press, 2017)

● **Articles Blogs**

1. Abhinav Dalal et al., “Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases, U. Chi. Legal Forum (Reimagining National Security)” (2025), <https://legal-forum.uchicago.edu/print-archive/deepfakes-court-how-judges-can-proactively-manage-alleged-ai-generated-material>. (Accessed: 03 March 2026).
2. Kent, K. et al. (2006) Guide to integrating forensic techniques into incident response, CSRC. Available at: <https://csrc.nist.gov/pubs/sp/800/86/final> (Accessed: 03 March 2026).
3. Mason, S., & Seng, D. (Eds.). (2017). Front Matter. In Electronic Evidence (4th ed., pp. i–vi). University of London Press. <http://www.jstor.org/stable/j.ctv512x65.1>
4. McCarthy, J. et al. (no date) A proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955, AI Magazine. Available at: <https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904> (Accessed: 05 March 2026).
5. Association for the Advancement of Artificial Intelligence, “Welcome to AAAI”



- <<https://www.aaai.org>> accessed 1 February 2026.
6. Rumelhart, D.E., Hinton, G.E. and Williams, R.J. (no date a) Learning representations by back-propagating errors, Nature News. Available at: <https://www.nature.com/articles/323533a0> (Accessed: 05 March 2026).
 7. Krizhevsky, A., Sutskever, I. and Hinton, G.E. (2012) Imagenet classification with deep convolutional neural networks. advances in neural information processing systems, 25, 1097-1105. <https://papers.nips.cc/paper/2020/hash/1457c0d6bfc4967418bfb8ac142f64a-Abstract.html> (Accessed:05 March 2026)
 8. Brown, T. et al. (1970) Language models are few-shot learners, Advances in Neural Information Processing systems <https://papers.nips.cc/paper/2020/hash/1457c0d6bfc4967418bfb8ac142f64a-Abstract.html>
 9. Ai Deception: A survey of examples, risks, and potential solutions. Available at: <https://arxiv.org/pdf/2308.14752> (Accessed: 05 March 2026).
 10. UN Secretary-General's High-level Advisory Body on Artificial Intelligence, Governing AI for Humanity: Final Report (United Nations, September 2024) [https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf] [04 March, 2026]
 11. Commission signed the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, democracy and the rule of law Shaping Europe's digital future. Available at: <https://digital-strategy.ec.europa.eu/en/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights> (Accessed: 04 March 2026).
 12. Singapore's Digital & AI Governance: A Pro-Innovation, Framework-Driven Model, accessed March 4, 2026, <https://blogs.duanemorris.com/duanemorrisandselvam/2026/03/03/singapores-digital-ai-governance-a-pro-innovation-framework-driven-model/>
 13. Guide to the protocols and use of AI in Australian Courts - Smokeball, accessed March 4, 2026, <https://www.smokeball.com.au/blog/guide-to-the-court-protocols-on-ai-in-australian-courts>
 14. China Releases New Labeling Requirements for AI-Generated Content - Inside Privacy, accessed March 4, 2026, <https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/>