Dispute Resolution and Knowledge Management

ALERT | 4 November 2025

In this issue

SOUTH AFRICA

AI, deepfakes and the burden of proof for digital evidence in litigation

For more insight into our expertise and services

DISPUTE RESOLUTION AND KNOWLEDGE MANAGEMENT ALERT

AI, deepfakes and the burden of proof for digital evidence in litigation

In 2022, a deepfake video circulated showing Ukrainian President Volodymyr Zelenskyy appearing to tell Ukrainian soldiers to surrender during the Russian invasion. Although quickly debunked, it demonstrated how synthetic media could be weaponised for geopolitical ends. The following year, Arup – the design company behind structures like the Sydney Opera House and the UK's Channel Tunnel Rail Link – lost USD 25 million after an employee was deceived by deepfake audio and video impersonating the UK-based CFO and other executives in a meeting, and convinced to transfer the money to the perpetrators.

The courtroom was an inevitable target. In September 2025, the Superior Court of California, County of Alameda was forced to impose terminating sanctions in *Mendones, et al v Cushman & Wakefield, Inc., et al* (Case No. 23CV028772) after finding that a video submitted as evidence by the plaintiffs was fabricated using artificial intelligence (AI), and then submitted as an authentic recording.

Although South African courts have not yet confronted a comparable case, the technology is widely accessible and our current evidentiary framework was drafted decades ago. Deepfakes were certainly not considered by policymakers.

What are deepfakes?

Deepfakes are AI-generated synthetic media, like images, audio and video, that create realistic but false representations of people doing or saying things they never did.

In the past, the most convincing deepfakes used autoencoder-based face swaps and then Generative Adversarial Networks (GANs) – a technology where two AI systems compete against each other. One creates fake content while the other tries to detect it, pushing both to improve until the fakes become nearly indistinguishable from reality. Today, technologies used for deepfakes include diffusion models and transformer-based architectures, sometimes producing even more realistic results than GANs alone, though typically with slower generation.

With time, more AI technology became available to the public and deepfake tools are now accessible to anyone with a laptop and free software. This means that a video of a person to be used as evidence, a recording of a party admitting fault, or footage contradicting an alibi can be altered or fabricated – or deepfaked – with relative ease.

How does South African law deal with electronic evidence today?

Section 15 of the Electronic Communications and Transactions Act 25 of 2002 (ECTA) establishes that "*data messages*" cannot be excluded as evidence merely because they are electronic. Courts must assess reliability by examining how the message was generated, stored and communicated; how its integrity was maintained; how its originator was identified; and any other relevant factors.

DISPUTE RESOLUTION AND KNOWLEDGE MANAGEMENT ALERT

AI, deepfakes and the burden of proof for digital evidence in litigation

CONTINUED

Under section 15(4), data messages made in the ordinary course of business (if properly certified) are admissible in evidence on production and constitute rebuttable proof of their contents.

Section 3 of the Law of Evidence Amendment Act 45 of 1988 (LEAA) governs hearsay, permitting admission as evidence when the interests of justice require it. Courts consider factors including the nature of the evidence and its probative value, the reason the original source is unavailable, and the potential prejudice to the parties.

Together, these provisions, along with the common law and process statutes, create a flexible, framework that admits digital evidence while demanding judicial scrutiny of reliability. But both statutes predate deepfakes by decades and they were promulgated when the primary concern was whether a fax or an email constituted credible evidence, not whether a video recording depicts reality at all.

How do you authenticate electronic evidence?

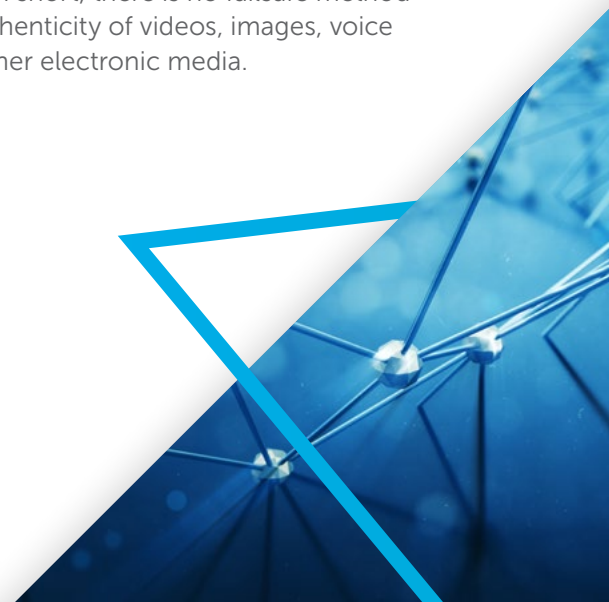
Traditional authentication methods include chain of custody documentation, metadata analysis, and witness testimony. Deepfakes undermine all of these.

A forensic analyst can only testify that certain artefacts were found on a device and, if the chain of custody is intact, that they weren't placed there after the collection was done. They cannot, however, always confirm how artefacts might have been placed on a device and whether the contents or metadata are a true reflection of reality. For example, if a person claims that artefacts were placed on their device by a stranger who loaned them their charging cable at the airport, without a corroborating witness, a forensic analyst's evidence would not be of assistance.

And this is how the technology creates two authentication failures:

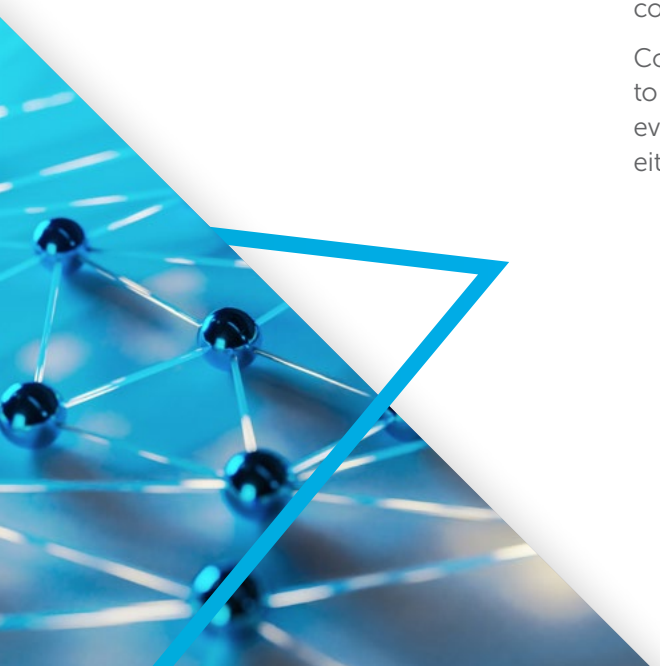
- **False positives:** A fabricated video may pass traditional scrutiny and be admitted as genuine. If the metadata is intact, the chain of custody documented, and the content facially plausible, courts and litigants may struggle to identify sophisticated fakes due to a lack of tools needed for this purpose.
- **False negatives:** Authentic evidence risks rejection whenever a party claims deepfake manipulation. This has already surfaced in cases like *Sz Huang et al v Tesla, Inc. et. al.* (Case No. 19CV346663), where Tesla's counsel refused to admit video evidence of Elon Musk on grounds it could easily have been deepfaked, especially because Musk is famous, and despite the absence of actual evidence of manipulation.

Technical detection tools do exist, but they are expensive, often require expert testimony and remain vulnerable to the same adversarial techniques that create deepfakes in the first place. In short, there is no failsafe method to confirm the authenticity of videos, images, voice recordings and other electronic media.



AI, deepfakes and the burden of proof for digital evidence in litigation

CONTINUED



How does this impact the burden of proof?

The party relying on electronic evidence bears the responsibility of proving authenticity. In the deepfake era, that burden becomes substantially heavier. Litigants may now need digital forensic experts simply to establish what was once obvious from the face of a recording. This drives up costs and complexity, creating a barrier to justice for smaller litigants and making certain claims uneconomical to pursue.

The reverse problem is equally problematic. Parties facing damaging but authentic evidence can deploy the 'deepfake defence' to manufacture doubt where none should exist. Recordings that would have been devastating in the past may now be called into question with a bare allegation of manipulation, forcing the tendering party to prove the authenticity of such recordings or a court to dismiss the evidence. In the *Tesla* case, the court ordered the deposition of Musk which, of course, would delay the conclusion of proceedings.

Courts face an unenviable task: having enough scepticism to guard against sophisticated fakes, but not so much that every video becomes presumptively suspect. Get it wrong either way and the consequences could be serious.

Why do the existing rules regarding evidence need to be adapted?

South African law's current technology-neutral stance is no longer sufficient. While the ECTA and LEAA allow flexibility, they do not contain any presumptions relating to evidence that may be synthetic or AI-generated, require early disclosure of whether AI tools were used in the creation of the evidence, or provide standards for expert testimony on digital authenticity.

Comparative jurisdictions are moving ahead. The Federal Rules of Evidence Advisory Committee in the US is actively considering amendments to address the authentication and admissibility of AI-generated content. A new proposed Federal Rule of Evidence 707 ("*Machine-Generated Evidence*") was approved by the Judicial Conference in June 2025 and is open for public comment until February 2026. This rule requires that AI-generated evidence must meet the same standards of reliability and admissibility under Rule 702 (which governs expert testimony) when presented without an expert witness. It ensures rigorous scrutiny, requiring demonstration that AI output is based on sufficient facts and reliable methods, and is reliably applied to the case facts.

Another proposal aims to amend Rule 901 on authentication to specifically address deepfake and generative AI evidence. It introduces a burden-shifting framework where a party challenging AI-manipulated evidence must provide sufficient proof that the content may be fabricated or altered by AI, placing the burden on the proponent to disprove authenticity.

AI, deepfakes and the burden of proof for digital evidence in litigation

CONTINUED

How can South Africa reform its existing legal framework?

Drawing on foreign practice and the realities of modern litigation, several reforms are worth considering:

- **Mandatory disclosure of AI involvement:** Parties should be required to disclose whether evidence has been created or altered using AI technologies. This places the burden of transparency on the party with knowledge of how the material was generated.
- **Enhanced authentication standards for audiovisual evidence:** Courts should demand more than facial plausibility before admitting video or audio recordings. Metadata analysis, chain of custody documentation, witness corroboration and expert testimony should become standard rather than exceptional requirements.
- **Understanding of the limits on digital authentication:** Courts should be well advised to consider that there is currently no robust mechanism to authenticate the origin of digital artefacts
- **Accredited digital forensic experts:** A recognised register of qualified forensic analysts would help courts and litigants distinguish between genuine, reliable experts and opportunistic or under-qualified practitioners. This could be administered through existing professional bodies or the judiciary itself.
- **Judicial training and bench guides:** Following the US' example, South African courts could develop practical 'bench cards' for judges. These would function as reference guides on identifying deepfake risks, framing the right questions for experts, and weighing reliability factors under section 15 of the ECTA.
- **Early resolution of authenticity disputes:** Case management rules should require parties to raise authenticity challenges early, with disputes resolved in pre-trial conferences or through case management rather than at trial. This prevents ambush tactics, ensures forensic evidence can be properly prepared and tested, and reduces the impact on courts' resources.

What challenges does South Africa face?

- **Resource constraints:** Unlike US courts, South African courts may lack access to forensic expertise and detection tools.
- **Volume of litigation:** With already strained court rolls, additional evidentiary hearings will increase delays.
- **Risk of injustice:** Marginalised litigants may be least able to afford expert testimony, raising fairness concerns.

What can we expect until solutions are found?

Until reforms are enacted, litigants and courts face a difficult landscape. We can expect more frequent disputes over digital recordings, from WhatsApp voice notes to CCTV footage. Courts and litigants will be increasingly forced to rely on costly – but potentially still refutable – expert evidence, and even then, they would need to take a considered view that audiovisual and digital artefacts can only add to the weight of circumstantial evidence as opposed to treating these artefacts as indisputable evidence. Most worryingly, there remains the potential for wrongful outcomes where deepfakes are admitted or genuine evidence is discredited.

AI, deepfakes and the burden of proof for digital evidence in litigation

CONTINUED

Conclusion

Deepfakes undermine the foundational assumption that audiovisual evidence depicts reality. South African law provides a relatively flexible baseline through the ECTA and LEAA, but neither statute was designed with synthetic media in mind.

Litigants should anticipate heavier evidentiary burdens when tendering video or audio recordings. Where authenticity is likely to be contested, early engagement with digital forensic experts will be necessary. On the other side, parties facing suspicious evidence should raise authenticity challenges promptly rather than waiting until trial.

Policymakers and the legislature and the judiciary will need to adapt procedural rules and evidentiary standards, learning from jurisdictions already grappling with these issues. Awareness should be raised with the judiciary, which will inevitably have to deal with these evidentiary challenges. For now, practitioners should work on the assumption that any digital recording can be challenged and trust that our courts are able to balance appropriate scepticism against the risk of rendering audiovisual evidence effectively inadmissible.

Safee-Naaz Siddiqi, Rynhardt Haarhof, Anja Hofmeyr and Annemari Krugel

OUR TEAM

For more information about our Dispute Resolution practice and services in South Africa, Kenya and Namibia, please contact:

Rishaban Moodley
Practice Head & Director:
Dispute Resolution
Sector Head:
Gambling & Regulatory Compliance
T +27 (0)11 562 1666
E rishaban.moodley@cdhlegal.com

Tim Fletcher
Chairperson
Director: Dispute Resolution
T +27 (0)11 562 1061
E tim.fletcher@cdhlegal.com

Patrick Kauta
Managing Partner | Namibia
T +264 833 730 100
M +264 811 447 777
E patrick.kauta@cdhlegal.com

Imraan Abdullah
Director:
Dispute Resolution
T +27 (0)11 562 1177
E imraan.abdullah@cdhlegal.com

Timothy Baker
Director:
Dispute Resolution
T +27 (0)21 481 6308
E timothy.baker@cdhlegal.com

Eugene Bester
Director:
Dispute Resolution
T +27 (0)11 562 1173
E eugene.bester@cdhlegal.com

Neha Dhana
Director:
Dispute Resolution
T +27 (0)11 562 1267
E neha.dhana@cdhlegal.com

Denise Durand
Director:
Dispute Resolution
T +27 (0)11 562 1835
E denise.durand@cdhlegal.com

Claudette Dutilleux
Director:
Dispute Resolution
T +27 (0)11 562 1073
E claudette.dutilleux@cdhlegal.com

Jackwell Feris
Sector Head:
Industrials, Manufacturing & Trade
Director: Dispute Resolution
T +27 (0)11 562 1825
E jackwell.feris@cdhlegal.com

Nastascha Harduth
Sector Head: Corporate Debt,
Turnaround & Restructuring
Director: Dispute Resolution
T +27 (0)11 562 1453
E n.harduth@cdhlegal.com

Anja Hofmeyr
Director:
Dispute Resolution
T +27 (0)11 562 1129
E anja.hofmeyr@cdhlegal.com

Annemari Krugel
Director:
Dispute Resolution
T +27 (0)11 562 1709
E annemari.krugel@cdhlegal.com

Mercy Kuzeeko
Director:
Dispute Resolution
T +26 (4)83 373 0100
E mercy.kuzeeko@cdhlegal.com

Corné Lewis
Director:
Dispute Resolution
T +27 (0)11 562 1042
E corne.lewis@cdhlegal.com

Nomlayo Mabhena-Mlilo
Director:
Dispute Resolution
T +27 (0)11 562 1743
E nomlayo.mabhena@cdhlegal.com

Sentebale Makara
Director:
Dispute Resolution
T +27 (0)11 562 1181
E sentebale.makara@cdhlegal.com

Vincent Manko
Director:
Dispute Resolution
T +27 (0)11 562 1660
E vincent.manko@cdhlegal.com

Khaya Mantengu
Director:
Dispute Resolution
T +27 (0)11 562 1312
E khaya.mantengu@cdhlegal.com

Richard Marcus
Director:
Dispute Resolution
T +27 (0)21 481 6396
E richard.marcus@cdhlegal.com

Lebogang Makwela
Director:
Dispute Resolution
T +27 (0)11 562 1057
E lebogang.makwela@cdhlegal.com

Burton Meyer
Director:
Dispute Resolution
T +27 (0)11 562 1056
E burton.meyer@cdhlegal.com

Desmond Odhiambo
Partner | Kenya
T +254 731 086 649
+254 204 409 918
+254 710 560 114
E desmond.odhiambo@cdhlegal.com

Lucinde Rhoodie
Director:
Dispute Resolution
T +27 (0)21 405 6080
E lucinde.rhoodie@cdhlegal.com

Clive Rumsey
Sector Head: Construction & Engineering
Director: Dispute Resolution
T +27 (0)11 562 1924
E clive.rumsey@cdhlegal.com

Belinda Scriba
Director:
Dispute Resolution
T +27 (0)21 405 6139
E belinda.scriba@cdhlegal.com

Tim Smit
Sector Head:
Consumer Goods, Services & Retail
Director: Dispute Resolution
T +27 (0)11 562 1085
E tim.smit@cdhlegal.com

Marelise van der Westhuizen
Director:
Dispute Resolution
T +27 (0)11 562 1208
E marelise.vanderwesthuizen@cdhlegal.com

Joe Whittle
Director:
Dispute Resolution
T +27 (0)11 562 1138
E joe.whittle@cdhlegal.com

Roy Barendse
Executive Consultant:
Dispute Resolution
T +27 (0)21 405 6177
E roy.barendse@cdhlegal.com

Rimo Benjamin
Counsel:
Dispute Resolution
T +27 (0)11 562 1716
E rimo.benjamin@cdhlegal.com

BBBEE STATUS: LEVEL ONE CONTRIBUTOR
Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

PLEASE NOTE
This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa.
Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

NAIROBI
Merchant Square, 3rd floor, Block D, Riverside Drive, Nairobi, Kenya. P.O. Box 22602-00505, Nairobi, Kenya.
T +254 731 086 649 | +254 204 409 918 | +254 710 560 114
E cdhkenya@cdhlegal.com

ONGWEDIVA
Shop No A7, Oshana Regional Mall, Ongwediva, Namibia.
T +264 (0) 81 287 8330 E cdhnamibia@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com

WINDHOEK
1st Floor Maerua Office Tower, Cnr Robert Mugabe Avenue and Jan Jonker Street, Windhoek 10005, Namibia.
PO Box 97115, Maerua Mall, Windhoek, Namibia, 10020
T +264 833 730 100 E cdhnamibia@cdhlegal.com

©2025 15282/NOV