INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

THE "DEEPFAKE DEFENSE": EVIDENTIARY CHALLENGES OF AUTHENTICATING AI-GENERATED AUDIO/VIDEO IN CRIMINAL TRIALS

AUTHORED BY - KHUSHI GUPTA & DR NIDHI SHARMA

Abstract

The emergence of sophisticated artificial intelligence capable of generating hyper-realistic synthetic audio and video—commonly referred to as "deepfakes"—poses an unprecedented challenge to the evidentiary framework of criminal proceedings. This paper examines the doctrinal and practical difficulties courts face when determining the authenticity of audio-visual evidence in an era where fabrication is indistinguishable to the naked eye. Drawing on existing rules of evidence, expert testimony standards, and emerging judicial responses, it argues that traditional authentication mechanisms are ill-equipped to address AI-generated media. The paper further considers the defendant's strategic deployment of the "deepfake defense"—challenging the authenticity of genuine prosecution evidence by raising the mere possibility of AI manipulation—and the risk this poses to wrongful acquittals. It concludes with proposals for doctrinal reform, including judicially endorsed technical standards, revised burdens of production, and legislative intervention to ensure the integrity of the truth-finding function in modern criminal trials.

1. Introduction

In 2019, a fabricated video of Belgian Prime Minister Sophie Wilmès circulated online, ostensibly linking climate change to COVID-19—a statement she never made.[1] The following year, a deepfake audio purporting to be a regional governor ordering his subordinates to commit fraud was used in a financial crime in the United Kingdom.[2] These incidents are not isolated curiosities. They are harbingers of an evidentiary crisis now arriving at the doors of criminal courts worldwide.

Deepfakes—a portmanteau of "deep learning" and "fake"—are synthetic media generated by artificial intelligence systems, particularly generative adversarial networks

[1]Nina Schick, *Deepfakes: The Coming Infocalypse* (Monoray 2020) 12.
[2]Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, 1758.

ISSN: 2582-6433

(GANs) and diffusion models, which can convincingly replicate the likeness, voice, and mannerisms of real individuals.[3] As these tools become widely accessible—commercially available applications now allow amateur users to create realistic deepfakes within minutes—the criminal justice system confronts a dual threat: (i) the admission of fabricated evidence by bad-faith actors, and (ii) the weaponisation of deepfake scepticism by defendants seeking to undermine genuine, unimpeachable evidence.

This paper proceeds as follows. Section 2 surveys the technical architecture of deepfake generation and detection. Section 3 examines the existing authentication framework under English law and analogous common law jurisdictions. Section 4 analyses the "deepfake defense" as a litigation strategy, with reference to emerging case law and scholarly commentary. Section 5 considers the role and limitations of expert testimony. Section 6 surveys comparative and international approaches. Section 7 proposes a framework for doctrinal and legislative reform. Section 8 concludes.

2. The Technology of Deception: Deepfakes and Detection

2.1 Generative Mechanisms

Deepfake technology primarily operates through two architectures. The first—and historically dominant—is the Generative Adversarial Network (GAN), introduced by Ian Goodfellow and colleagues in 2014.[4] A GAN pits two neural networks against each other: a "generator" that produces synthetic content, and a "discriminator" that attempts to detect fabrications. Through iterative competition, the generator learns to produce outputs that fool the discriminator with increasing fidelity. The second architecture—diffusion models—operates by learning to reverse a process of noise injection, enabling the production of highly photorealistic images and video from text prompts.[5]

The practical outputs of these systems are startling. Face-swap deepfakes substitute one individual's facial features onto another's body with near-perfect continuity of lighting and motion. Voice-cloning technology—now commercially available through platforms such as Eleven Labs and Resemble AI—can replicate a speaker's voice from as few as three seconds

[3]Hao Li and others, 'Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics' (2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle 2020).
[4]Ian Goodfellow and others, 'Generative Adversarial Nets' (2014) 27 Advances in Neural Information Processing Systems 2672.
[5]Jonathan Ho, Ajay Jain and Pieter Abbeel, 'Denoising Diffusion Probabilistic Models' (2020) 33 Advances in Neural Information Processing Systems 6840.

ISSN: 2582-6433

of audio.[6] Lip-sync deepfakes synchronise fabricated audio with a target's pre-existing video, creating the appearance of utterances never made.

2.2 The Detection Problem

Detection methodologies have developed in parallel with generative techniques, though with persistent asymmetry—generative models consistently outpace their forensic counterparts. Current detection approaches fall into three broad categories.

First, artefact-based detection identifies the residual inconsistencies left by generative algorithms: irregular blinking patterns, inconsistent lighting, spectral anomalies in the frequency domain, and physiological implausibilities such as the absence of pulse-driven skin colour variation.[7] Second, watermarking and provenance verification mechanisms embed cryptographic signatures into genuine media at the point of capture, enabling downstream verification of integrity.[8] Third, physiological signal analysis exploits the fact that human faces carry subtle, spatially consistent bio-signals—imperceptible micro-expressions, vasomotor responses—that current generative models fail to replicate convincingly.[9]

Critically, each of these methods is fallible. Detection accuracy in laboratory settings—often exceeding 95%—degrades substantially in adversarial conditions, with compressed video (the standard format for social media and messaging applications) and with next-generation generative models specifically trained to evade known detectors.[10] The National Institute of Standards and Technology (NIST) has acknowledged that no current detection methodology achieves the reliability standards generally expected of forensic evidence in legal proceedings.[11]

3. The Authentication of Audio-Visual Evidence: Existing Doctrine

3.1 The General Requirement of Authentication

Authentication—the process by which the proponent of evidence satisfies the tribunal that the evidence is what it purports to be—lies at the foundation of the law of evidence. In

[6]Europol Innovation Lab, 'Facing Reality? Law Enforcement and the Challenge of Deepfakes' (Europol 2022) 9.
[7]David Guera and Edward Delp, 'Deepfake Video Detection Using Recurrent Neural Networks' (2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance, Auckland 2018).
[8]Hany Farid, 'Image Forgery Detection' (2009) 26 IEEE Signal Processing Magazine 16, 23.
[9]Xuaner Zhang and others, 'FakeCatcher: Detection of Synthetic Portrait Videos using Biological Signals' (2022) 45 IEEE Transactions on Pattern Analysis and Machine Intelligence 1.
[10]Davide Cozzolino and others, 'Towards Universal Fake Image Detection Probing the Limits of Existing Academia and Industry Models' (2023) IEEE/CVF Conference on Computer Vision and Pattern Recognition.
[11]National Institute of Standards and Technology, 'Deepfake Detection Challenge: Insights and Next Steps' (NIST 2021) 4.

ISSN: 2582-6433

England and Wales, no single statutory provision comprehensively governs the authentication of electronic evidence, though the Police and Criminal Evidence Act 1984 (PACE) and the Criminal Justice Act 2003 provide the relevant statutory framework for documentary and hearsay evidence.[12]

At common law, authentication of audio-visual evidence requires the proponent to adduce sufficient evidence from which a reasonable jury could conclude that the recording is what it purports to be.[13] This may be achieved through witness testimony identifying the recording's content, evidence of chain of custody, technical evidence regarding the integrity of the recording medium, or some combination thereof. In the United States, Federal Rule of Evidence 901 codifies a functionally identical requirement, providing that the proponent must produce "evidence sufficient to support a finding that the item is what the proponent claims it is."[14]

3.2 Electronic Evidence and the Presumption of Reliability

English courts have historically approached computer-generated evidence with a degree of suspicion subsequently tempered by statute. Section 69 of PACE 1984, which required affirmative proof that a computer was operating correctly, was repealed by the Youth Justice and Criminal Evidence Act 1999, effectively introducing a presumption that computers operate reliably absent specific evidence to the contrary.[15]

This presumption has been criticised as increasingly unrealistic in the context of AI-generated media. Professor Paul Roberts has argued that the legislative elimination of the Section 69 safeguard predated the widespread deployment of adversarial generative models and should be revisited in light of current forensic realities.[16]

3.3 The Standard for Admissibility versus Weight

A critical distinction pervades authentication doctrine: the difference between admissibility and weight. In England and Wales, the admissibility threshold—whether the jury may consider the evidence at all—is relatively low; once basic authentication is satisfied, the question of how much weight to attach to the evidence is for the jury. In practice, this

[12]Police and Criminal Evidence Act 1984, s 69 (repealed); Civil Evidence Act 1995; Criminal Justice Act 2003, ss 114–136.
[13]*R v Robson* [1972] 1 WLR 651 (Crown Court); *R v Flynn and St John* [2008] EWCA Crim 970, [2008] 2 Cr App R 20.
[14]Federal Rules of Evidence, Rule 901(a).
[15]Youth Justice and Criminal Evidence Act 1999, s 60; *R v Shephard* [1993] AC 380 (HL).
[16]Paul Roberts and Adrian Zuckerman, *Criminal Evidence* (3rd edn, OUP 2022) 481–483.

ISSN: 2582-6433

bifurcation creates difficulty where the authenticity challenge is probabilistic rather than categorical: a defendant who argues that evidence "might" be a deepfake does not necessarily contest admissibility outright, but rather invites the jury to treat the evidence as unreliable.[17]

4. The "Deepfake Defense" in Criminal Proceedings

4.1 Anatomy of the Defense

The "deepfake defense" denotes a litigation strategy whereby a defendant challenges prosecution audio-visual evidence—or, less commonly, exculpatory evidence of their own—on the basis that it has been artificially generated or manipulated. Its deployment takes several forms. In its strongest form, the defense presents expert evidence that specific technical artefacts within the impugned recording are consistent with AI synthesis. In its weakest—and most legally controversial—form, the defense merely invokes the general possibility that deepfakes exist and are technologically feasible, without identifying specific indicia of manipulation in the impugned material.

The latter strategy exploits what legal scholars have termed the "liar's dividend": the phenomenon whereby the mere existence of deepfake technology undermines public trust in genuine audio-visual evidence, regardless of whether any specific fabrication has occurred.[18] As Chesney and Citron observe, the liar's dividend is in certain respects more socially corrosive than deepfakes themselves, because it benefits bad actors who can deny authentic recordings simply by gesturing at technological possibility.

4.2 Emerging Judicial Encounters

While the deepfake defense has not yet produced a definitive appellate ruling in English law, its precursor—challenges to CCTV and digital recordings on grounds of manipulation—has generated instructive authority. In *R v Riat*, the Court of Appeal emphasised that reliability challenges to electronically stored documents require particularised evidential foundation, not mere assertion.[19]

In the United States, the deepfake defense has begun to appear with increasing frequency. In *United States v Safavian*, the court held that challenges to electronic evidence authenticity require a prima facie showing beyond speculative possibility.[20] More directly, in

[17] *R v Taylor* [2006] EWCA Crim 260; Mike Redmayne, *Expert Evidence and Criminal Justice* (OUP 2001) 133.
[18] Chesney and Citron (n 2) 1800–1801.
[19] *R v Riat* [2012] EWCA Crim 1509, [2013] 1 WLR 2592 [15] (Hughes LJ).
[20] *United States v Safavian* 435 F Supp 2d 36 (DDC 2006) 40–41.

ISSN: 2582-6433

a 2023 Maryland case, a defendant sought to exclude recorded statements by alleging, without expert support, that they constituted deepfakes; the court rejected the challenge as speculative.[21]

In the English context, the Crown Prosecution Service Guidance on Digital Evidence recognises the theoretical risk of manipulated recordings but does not yet prescribe standardised authentication protocols specifically directed at AI-generated content.[22]

4.3 Burden and Standard of Proof

The allocation of the burden of proof in deepfake challenges is contested. On orthodox principles, the prosecution bears the legal burden of proving each element of its case beyond reasonable doubt, and authentication of its own evidence is an implicit component of that burden. The defendant, presenting the deepfake defense, bears no legal burden—it suffices to raise a reasonable doubt.[23]

However, scholars including Professor Jenny McEwan have argued that the orthodox position requires modification where the defendant deploys a technological defense that they alone have the capacity to substantiate.[24] Drawing on the "reverse burden" jurisprudence under the Human Rights Act 1998 and Article 6 of the European Convention on Human Rights, it may be argued that where a defendant alleges fabrication of prosecution evidence through technologically sophisticated means, they bear at least an evidential burden—a burden of production—to adduce some particularised basis for the allegation.[25]

5. Expert Testimony and Its Limitations

5.1 Admissibility of Expert Evidence

Expert evidence on the authenticity of audio-visual recordings is admissible in English criminal proceedings where it satisfies the general test set out in *R v Bonython*: the subject matter must be one upon which expert opinion is necessary and the witness must be sufficiently skilled.[26] The Law Commission's 2011 report on expert evidence recommended a formal reliability gatekeeping criterion—analogous to the United States' Daubert standard—which was not legislatively implemented but has influenced judicial practice.[27]

[21]State v *Malik* (Circuit Court, Prince George's County 2023) unreported, discussed in Paul W Grimm, 'Authentication of Digital Evidence' (2023) 45 American Journal of Trial Advocacy 1.
[22]Crown Prosecution Service, *Digital Evidence Guidance* (CPS 2023) <https://www.cps.gov.uk/digital-evidence> accessed 12 March 2025.
[23]*Woolmington v DPP* [1935] AC 462 (HL).
[24]Jenny McEwan, *Evidence and the Adversarial Process: The Modern Law* (2nd edn, Hart 1998) 267.
[25]*R v Lambert* [2001] UKHL 37, [2002] 2 AC 545; Human Rights Act 1998, s 3.
[26]*R v Bonython* (1984) 38 SASR 45, adopted in England in *R v Robb* (1991) 93 Cr App R 161.
[27]Law Commission, *Expert Evidence in Criminal Proceedings in England and Wales* (Law Com No 325, 2011)

ISSN: 2582-6433

In deepfake authentication, the relevant expert disciplines include digital forensics, machine learning, and signal processing. Courts in England and Wales have admitted testimony from digital forensic analysts on the integrity of digital recordings in cases involving allegations of manipulation,[28] though the specific field of AI-generated media forensics has not yet been tested before a senior appellate tribunal.

5.2 The Reliability Gap

The central limitation of expert evidence in this context is the absence of validated, standardised detection methodologies. Unlike DNA profiling—where the Population Genetics Committee, the Forensic Science Regulator, and the ENFSI have established validated probabilistic protocols—deepfake detection operates without regulatory accreditation or agreed error-rate benchmarks.[29] The absence of such frameworks makes it difficult for courts to assess the probative value of expert detection opinions and impossible to present the evidence in the form of likelihood ratios familiar from forensic science practice.

Professor Norman Siebrasse has observed that courts risk falling into two symmetrical errors: over-crediting detection evidence that is not robustly validated, or under-crediting it by demanding standards of certainty that no available methodology can provide.[30]

5.3 The "Battle of the Experts" Problem

Where both prosecution and defense adduce expert testimony on the authenticity of the same recording—each expert offering diametrically opposed conclusions—the jury is ill-positioned to adjudicate between them. The Runciman Commission observed that contested scientific evidence presented through adversarial expert testimony systematically risks confusing rather than enlightening the fact-finder.[31] This concern is amplified in the deepfake context, where the underlying technology is opaque even to technically literate observers, and where the relevant empirical claims are inherently probabilistic.

paras 1.22–1.30; *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US 579 (1993).
[28]*R v Clinton* [2012] EWCA Crim 2, [2012] 1 WLR 1542.
[29]Forensic Science Regulator, *Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System* (FSR-C-100, Issue 7, 2021) ch 23.
[30]Norman Siebrasse, 'The Admissibility of AI-Generated Evidence' (2022) 85 Modern Law Review 1243, 1259.
[31]Royal Commission on Criminal Justice, *Report* (Cm 2263, HMSO 1993) ch 9, para 63.

ISSN: 2582-6433

6. Comparative and International Perspectives

6.1 The United States

The United States presents the most developed body of authority on digital evidence authentication. Under Federal Rule of Evidence 901(b)(9), process or system evidence may be authenticated by "describing a process or system and showing that it produces an accurate result." The *Daubert* standard governs the admissibility of expert detection testimony, requiring that the methodology be grounded in sufficient facts or data, be the product of reliable principles and methods, and be reliably applied to the facts of the case.[32]

Several US states have enacted legislation directly addressing deepfakes. California's AB 602 and AB 730 (2019) target the use of deepfakes in pornography and political advertising respectively,[33] while Virginia and Georgia have enacted criminal provisions.[34] No US federal legislation has yet specifically addressed deepfake evidence in criminal proceedings, though the DEEPFAKES Accountability Act has been introduced in successive Congressional sessions without passage.

6.2 The European Union

The European Union's approach has been primarily regulatory rather than evidentiary. The AI Act (Regulation (EU) 2024/1689), adopted in 2024, imposes transparency obligations on providers of AI systems capable of generating synthetic audio-visual content, including mandatory disclosure labelling.[35] While these obligations do not directly govern criminal evidence, they create a regulatory infrastructure of provenance verification that could, in principle, be leveraged in forensic authentication.

6.3 India and the Global South

India presents a particularly acute challenge. The Information Technology Act 2000 and the Indian Evidence Act 1872, as amended, provide the framework for electronic evidence, but make no provision for AI-generated synthetic content.[36] The 2022 Parliamentary Standing Committee on Communications and Information Technology flagged deepfakes as a growing law enforcement concern, though no legislative response has followed. Given India's vast

[32] *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US 579 (1993) 597.
[33] California Assembly Bill 602 (2019); California Assembly Bill 730 (2019).
[34] Virginia Code Ann § 18.2–386.2; Georgia Code Ann § 16-11-90.
[35] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, art 50.
[36] Information Technology Act 2000 (India), s 65B; Indian Evidence Act 1872, s 45A (inserted by IT Act 2000).

ISSN: 2582-6433

digital population and the rapid proliferation of affordable deepfake tools, the gap between regulatory intent and doctrinal capacity is particularly pronounced.

7. Proposals for Doctrinal and Legislative Reform

7.1 A Particularised Pleading Requirement

Courts should require that defendants raising the deepfake defense discharge an evidential burden—a burden of production—sufficient to demonstrate a prima facie, particularised basis for believing that the impugned evidence has been artificially generated or manipulated. This would require specific identification of technical artefacts, inconsistencies, or chain-of-custody failures, rather than mere invocation of the general feasibility of deepfake technology. Such a requirement is consistent with the approach in *Riat* and would mirror the pleading standards applied to other forensic challenges under Criminal Procedure Rule 19.[37]

7.2 A Forensic Science Regulator Protocol

The Forensic Science Regulator should develop a validated protocol for the authentication of audio-visual evidence suspected of deepfake manipulation, analogous to existing protocols for digital image analysis. Such a protocol should define minimum methodological requirements for detection tools admitted as expert evidence, establish error-rate benchmarks, and mandate disclosure of the specific algorithmic tools and training datasets employed.[38]

7.3 A Statutory Content Provenance Framework

Parliament should enact legislation requiring manufacturers of professional recording devices, and platforms hosting audio-visual evidence used in criminal proceedings, to implement C2PA (Coalition for Content Provenance and Authenticity) compliant metadata standards, enabling courts to verify the provenance of recordings through cryptographic chain-of-custody.[39]

7.4 Judicial Training and Specimen Directions

The Judicial College should develop specimen jury directions addressing deepfake

[37] *R v Riat* (n 19); Criminal Procedure Rules 2020 (SI 2020/759), r 19.3.
[38] Forensic Science Regulator Act 2021; Forensic Science Regulator, *Guidance: Validation of Analytical Methods for Forensic Science Laboratories* (FSR-G-201, 2020).
[39] Coalition for Content Provenance and Authenticity, *C2PA Technical Specification* v2.0 (C2PA 2024) <https://c2pa.org/specifications/specifications/2.0/specs/C2PA_Specification.html> accessed 12 March 2025.

ISSN: 2582-6433

evidence, ensuring that jurors understand both the possibility of synthetic media and the requirement that challenges to authenticity be grounded in specific evidence. The directions should caution against both uncritical acceptance of audio-visual evidence and speculative scepticism unsupported by the forensic record.[40]

8. Conclusion

The advent of generative artificial intelligence has fundamentally disrupted the evidentiary calculus upon which criminal courts have long relied. Audio-visual evidence—once regarded as among the most compelling and self-authenticating forms of proof—has become epistemically contested in ways that existing doctrine does not adequately address. The "deepfake defense", in its legitimate form, raises genuine questions of probative reliability; in its cynical form, it exploits technological uncertainty to undermine truthful evidence.

The response of courts and legislatures must be calibrated and proportionate. It must not suppress legitimate challenges to fabricated evidence—such challenges go to the heart of the right to a fair trial enshrined in Article 6 of the ECHR. But it must equally resist the erosion of the truth-finding function through evidence-free speculation. The proposals advanced in this paper—a particularised pleading requirement, a regulatory forensic protocol, a statutory provenance framework, and improved judicial directions—represent a coherent, workable foundation for that calibration.

The fundamental challenge, ultimately, is epistemic: in a world where seeing is no longer believing, criminal justice systems must develop institutional mechanisms for knowing. The integrity of the criminal trial depends upon it.

Bibliography

Cases

Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579 (1993)

R v Bonython (1984) 38 SASR 45

R v Clinton [2012] EWCA Crim 2, [2012] 1 WLR 1542

R v Flynn and St John [2008] EWCA Crim 970, [2008] 2 Cr App R 20

R v Lambert [2001] UKHL 37, [2002] 2 AC 545

R v Riat [2012] EWCA Crim 1509, [2013] 1 WLR 2592

[40]Judicial College, *Crown Court Compendium* (HMSO, updated 2024) ch 20.

ISSN: 2582-6433

R v Robb (1991) 93 Cr App R 161

R v Robson [1972] 1 WLR 651

R v Shephard [1993] AC 380

R v Taylor [2006] EWCA Crim 260

United States v Safavian 435 F Supp 2d 36 (DDC 2006)

Woolmington v DPP [1935] AC 462

Legislation

Artificial Intelligence Act (EU) 2024/1689

California Assembly Bill 602 (2019)

California Assembly Bill 730 (2019)

Criminal Justice Act 2003

Criminal Procedure Rules 2020 (SI 2020/759)

Federal Rules of Evidence (US)

Forensic Science Regulator Act 2021

Human Rights Act 1998

Information Technology Act 2000 (India)

Police and Criminal Evidence Act 1984

Youth Justice and Criminal Evidence Act 1999

Books

McEwan J, Evidence and the Adversarial Process: The Modern Law (2nd edn, Hart 1998)

Redmayne M, Expert Evidence and Criminal Justice (OUP 2001)

Roberts P and Zuckerman A, Criminal Evidence (3rd edn, OUP 2022)

Schick N, Deepfakes: The Coming Infocalypse (Monoray 2020)

Journal Articles

Chesney R and Citron D, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753

Farid H, 'Image Forgery Detection' (2009) 26 IEEE Signal Processing Magazine 16

Grimm PW, 'Authentication of Digital Evidence' (2023) 45 American Journal of Trial Advocacy 1

Siebrasse N, 'The Admissibility of AI-Generated Evidence' (2022) 85 Modern Law Review 1243

ISSN: 2582-6433

Official and Institutional Reports

Crown Prosecution Service, Digital Evidence Guidance (CPS 2023)

Europol Innovation Lab, Facing Reality? Law Enforcement and the Challenge of Deepfakes (Europol 2022)

Forensic Science Regulator, Codes of Practice and Conduct for Forensic Science Providers and Practitioners (FSR-C-100, Issue 7, 2021)

Judicial College, Crown Court Compendium (HMSO, updated 2024)

Law Commission, Expert Evidence in Criminal Proceedings in England and Wales (Law Com No 325, 2011)

National Institute of Standards and Technology, Deepfake Detection Challenge: Insights and Next Steps (NIST 2021)

Royal Commission on Criminal Justice, Report (Cm 2263, HMSO 1993)