



REFORMING SRI LANKAN LAW TO ADDRESS DEEP FAKES: ENSURING ADMISSIBILITY OF CONTEMPORANEOUS RECORDINGS IN EVIDENCE

Yashinda Bandara Dissanayake

Department of Legal Studies, Faculty of Humanities & Social Sciences, Open University, Nawala, Sri Lanka

ABSTRACT

The modern world has flourished with technological improvement and has developed a technology called “Deep-fake”, through deep learning algorithms. Deep-fake technology which has both benefits and harm, is a creation of artificial intelligence. While deep-fake can be used to talk to your deceased relation again, the technology can be used to manipulate the pictures, videos and audio recordings which can mislead the judiciary by tendering as evidence and an innocent may be imprisoned. At the same time, a criminal or civil offender will be released from law enforcement by using deep fakes by defrauding photo, video and audio recordings. The main objective of this scrutiny is to find out the gaps in the Sri Lankan legal regime in combatting such deep-faked contemporaneous recordings and their admissibility before the judiciary in technological and legal perception. The “black letter” methodology was used to conduct the research by referring to local legislations, research papers and books. The research also discussed the admissibility of contemporaneous recordings as evidence and the methods of authentication of such evidence. Moreover, the paper supplies a directive authority on laws to be enforced and legal remedies to mitigate rendering deep-fake illusions to courts and technological recommendations as well. The final result is that Sri Lankan law should be improved regarding the authentication of contemporaneous recordings before admission, changes have to be made to the presumptions on the admissibility of contemporaneous recordings as evidence and penal laws on the creating and immoral use of deep fakes, subject to exceptions mentioned in the recommendations.

KEYWORDS: Law on Artificial Intelligence, law of evidence, admissibility of evidence, deep-fake, proposed law

Corresponding Author: Yashinda Bandara Dissanayake, E mail: yashindad@gmail.com



<https://orcid.org/0009-0007-2094-2766>



This is an open-access article licensed under a Creative Commons Attribution 4.0 International License (CC BY), allowing distribution and reproduction in any medium, crediting the original author and source.

1. INTRODUCTION

In the present world, with technological development, the concept of Artificial Intelligence was first cited in the first half of the 20th century. The main objectives of Artificial Intelligence were to simplify human workload and other technologies, making lives easier through problem-solving, doing multiple tasks at once, analysing big data sets, performing more complex tasks and helping human beings with planning. With the modern flourishing of artificial intelligence, the technology of deep learning was introduced. Deep learning algorithms have invented deep fake. Despite the benefits, the harm of deep-fake technology is vast and has to be controlled by the legal authorities and the legislature by imposing relevant legislation and technological methods to fight against the immoral use of deep-fake technology. The ultimate objective of the law, namely “justice” would be quashed away by such technology through altering images, audio and videos under the context of evidence. An image, audio or video generally recognized in evidence law as contemporaneous recordings in its immoral usage would lead the courts to injustice without true knowledge of courts. This paper discusses technological remedies to counter deep-fake misleading. Under this view, the current methods of authentication of contemporaneous recordings in courts and relevant remedies are discussed to cater for the probable issue of deep-fake evidence. In addition, the changes that have to be made to evidence law and criminal law are discussed in the paper to fill the gap in current law relevant to the admissibility of contemporaneous recordings as evidence and fill the gap in criminal law to combat the immoral use of deep-fakes.

1.1 What is Artificial Intelligence?

In its literal meaning, Artificial Intelligence duplicates and develops human thoughts, vision and apparent actions by algorithms put into machines such as robotics and computers. Simply Artificial Intelligence is a simulation of human intelligence by machines. Most of the time the terms machine learning, Artificial Intelligence and deep learning are used interchangeably despite those terms being different. For simple reference, machine learning is a subset of

Artificial intelligence and deep learning is a subset of machine learning. (Dignum, 2019)

1.2 Deep- Fake Technology

Deepfake is an artificial intelligence system that uses neural network technology to splice individual noises, facial expressions, and body motions into fraudulent material. In simple terms, Deep-fake technology can imitate and predict the characteristics of a specific person in terms of behaviour, facial identity, voice and some aspects of insight of the person. Further, deep-fake technology in its literal meaning learning deeply through deep learning algorithms. After the placement of algorithms, the machine starts to learn from past experiences and circumstances to predict the future and act in the present. In the legal context, the term “deep-fake” is defined in the Malicious Deep Prohibition Act (a bill) of the United States as “an audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual”. Again the Bill of Defending each Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023 defines the term as

“any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof— “(A) which appears to authentically depict any speech or conduct of a person who did not 3 engage in such speech or conduct; and 4 “(B) the production of which was substantially dependent upon technical means, rather 6 than the ability of another person to physically 7 or verbally impersonate such person”.

1.3 Contemporaneous Recordings

In its literal sense, contemporaneous recordings are audio or visual recordings that are recorded at the same time the fact occurs. Visual recordings are video recordings recorded by cameras, cameras in mobile phones, closed circuit television (CCTV) or any other similar type of device. Audio recordings can be referred to as recordings recorded through a Dictaphone, mobile phone, telephone call recordings and any other similar device.

2. METHODOLOGY

The scrutiny is based on the information, data, and knowledge gathered primarily and secondarily from statutes, books, journal articles, and online written materials. A mixed method including the doctrinal methodology, international and comparative methodologies are used to conduct the research as the research takes an analysis while providing a directive measure for the legal framework Sri Lanka needs. The area of discussion completely depends on the existing legal framework and the ideal law that would fit the current needs. Evidence Law is completely written and the gaps and problems had to be found in such materials. As the technological remedies are written in the scholarly articles, the research was carried out under the doctrinal methodology. The paper discusses the legal framework that has to be imposed in Sri Lanka.

3. RESULTS AND DISCUSSION

3.1 General Principle of Admissibility of Evidence

Admissibility of evidence required two basic things namely relevance and the evidence must not be prohibited by an exclusionary rule (Chalmers). All the evidence may not be relevant to the facts in issue. The evidence which is logically connected with matters in dispute is considered relevant evidence. There are two types of relevant evidence namely direct and indirect evidence. Direct evidence proves or disproves the fact-in-issue itself while indirect evidence supports the conclusion of the fact whether the fact proved, disproved or not proved. Exclusionary rules such as the hearsay rule which is generally excluded by law, unreliability, misleading, evidence against public policy and unnecessary are not admitted before the courts as evidence. In Sri Lanka, the evidence must be regarding a fact in issue or a relevant fact.

3.2 Current Methods of Authentication of Contemporaneous Recordings

In terms of photographs, videos or audio recordings authentication is an important factor in the admissibility of such contemporaneous recordings. Courts typically admit photographic evidence or evidence under one of two theories called “Pictorial Testimony Theory” and “Silent Witness” theory

(LaMonaga and P, vol. 69). Courts commonly consider photographic evidence as illustrative evidence rather than substantive evidence. In this sense, the photo evidence can be brought to the courts to illustrate the oral testimony of the witness. This theory suggests that photographic evidence is merely a graphic portrayal which supplements the oral evidence of the witness when considered under the pictorial testimony theory. The authentication is merely based on the knowledge of the witness regarding what the evidence is best of the knowledge and belief of the witness as per section 6(2) of ESPA. On the other hand, the Silent Witness theory supplies evidence as substantive evidence where a photograph or a video stands for its depiction. Simply under the silent witness theory, contemporaneous recordings are considered an independent source of information to prove a fact. In such a case, the proponent has to establish the authenticity of the evidence submitted. However, the presumption enumerated in Section 9 of the ESPA still traverses the authentication responsibility over the person who submits the contemporaneous recording as evidence. Nowadays, the most common methods of silent witnesses are CCTV footage, mobile phone videos, photographs, audio recordings and similar recordings.

3.3 Relevant Laws on Admissibility of Contemporaneous Recordings

The evidence and the law of evidence have different meanings. The term “Evidence” is a creation of the Latin term “Evidentia” which means to show, ascertain and prove something. Evidence law is an important part of the law as an adjective law which bridges substantial and procedural laws respectively providing rights, duties and liabilities of anyone against another. This means the statute that establishes the legal framework for put substantive law into effect and upholding it. The procedural law provides the procedure to carry out such substantial laws. Considering the aims of Evidence Law, the predominant objective is to regulate the process of proof of facts for legal proceedings (Dennis, 2020).

The Sri Lankan Evidence Law is primarily based on The Evidence Ordinance of 1895 in which section 5 of the said Ordinance states that evidence can be given

only regarding facts in issue and relevant facts. Section 3 defines Evidence as all statements which the court permits or requires to be made before it by witnesses about matters of facts under inquiry which is called oral evidence and the other mode of evidence is documentary evidence defined as all documents that are for the inspection of courts. The interpretation of the term “document” is also stated in the principal enactment as any matter expressed or described upon any substances employing letters, figures or marks or by more than one of these, intended to be used, to record the matter. It is evident that even from the very olden days, Courts in Sri Lanka were very much inclined to admit and rely upon the evidence which has been generated with the assistance of technology, even though such evidence did not appear on a surface similar to a sheet of paper (*Marine Star(Pvt)Ltd. vs. Amanda Foods Lanka (Pet) Ltd, [2008]*).

Until the impact of the case of *Benwell v. Republic of Sri Lanka*, the legislature did not tend to amend the principal enactment to make computer-stored data or information considered evidence. After the case, the Evidence (Special Provisions) Act of 1995 was established as a separate legislation from the Evidence Ordinance to make computer evidence and contemporaneous recordings admissible before courts. However, despite the evidence ordinance has made proving the facts in issue, based its entirety on oral and documentary evidence, there were some cases where the courts admitted contemporaneous recordings of public speeches and audio telephone call recordings. At present, after the enforcement of the Evidence (Special Provisions) Act contemporaneous recordings are admitted by courts as evidence according to section 4(1) of ESPA. Section 4(1) states that where direct oral evidence is admissible, any contemporaneous recordings or reproduction thereof can be brought to establish that oral evidence. Such recordings or reproductions must be made by using an electronic or mechanical device, the recording must be capable of being played, replayed, displayed or reproduced in a manner that can be perceived by the senses, the machine which made the recording must be operated properly at the time of recording reproducing of displaying, and the recording must not be tampered or altered.

Part one (1) of the Evidence (Special Provisions) Act of 1995 deals with the admissibility of contemporaneous recordings created using mechanical or electronic devices. This type of evidence has been categorized under real evidence which is opposed to oral or documentary evidence. Even though the Evidence Ordinance defines evidence as oral and documentary, the proviso to section 60 of the Evidence Ordinance empowers the admissibility of any other material thing as evidence other than a document where the court thinks it is fit. Section 165 of the Evidence Ordinance says the judge has discretionary power to order to submission of a document or a “thing” whether relevant or irrelevant.

Part three of the Evidence (Special Provisions) Act of 1995 (ESPA) sets out the procedure of tendering evidence under Sections 4 and 5 which are respectively on contemporaneous recordings and computer evidence. Accordingly, the Act provides provisions in section 6(1) to submit an affidavit on tendering such contemporaneous recordings or computer evidence in the first instance rather than summoning oral testimony of the maker of the affidavit. According to Section 6(2), any information in these affidavits would be sufficient if it is "stated to the best of the person stating its knowledge and belief." The proviso in this subsection states that the "Court may on application by the opposing party or of its motion, examine the maker of the affidavit, and or any other person said to be acquainted with any of the matters set out in the affidavit in open court touching any of the matters set out in the affidavit or any other relevant matter". Unlike the Criminal Procedure Code and the Civil Procedure Code, The ESPA by section 7 stipulates that contemporaneous recording or computer evidence shall be submitted before forty-five (45) days from the date of the trial. Similarly, the opposing party can inspect the computer evidence or contemporaneous recording and the machine that the evidence was made, within fifteen (15) days of receipt of such notice of the evidence as stated by section 7(1) (b) of ESPA. It is noteworthy the presumption stated in section 9 of the ESPA regarding the accuracy of the recording until proven to the contrary. In addition, the Electronic Transaction Act No.19 of 2006 in its section 21(2) stipulates that “Any information

contained in a data message, or any electronic document, electronic record or other communication— (a) touching any fact in issue or relevant fact and (b) compiled, received or obtained during any business, trade or profession or other regularly conducted activity, shall be admissible in any proceedings. Also, the same section accepts electronic records are accurate.

3.4 Impact of the Hearsay Rule

Hearsay is a statement originally made out of the courts. This is a statement which the witness repeated in the court according to the status of mind of the witness, on what they heard from another person. In other words, his/her evidence relates to something that has been seen, heard or perceived by someone else who is not called as evidence. The distinguishing between original and hearsay is primarily based on the originality of the witness. Even though the Evidence Ordinance is silent in this regard, the general rule is that hearsay is not admitted in both criminal and civil proceedings. The reason is such second-hand or third-hand evidence is not reliable (Cochran, Mary Ann Kelly and Gulycz, 2016) and the admissibility of such unreliable evidence is opposed to the general principles of admissibility of evidence. However, all the statements made out of the courts are not considered hearsay. Where such hearsay evidence was brought before the courts to prove the truth of the content, those kinds of evidence are not admissible as it is hearsay. Where the statement is not offered for its truth, it is not hearsay and can be admitted as evidence (Cochran, Mary Ann Kelly and Gulycz, 2016). It is worth pointing out the statement of the Privy Council on the appeal of the classic English case *Subramaniam V The Director of Public Prosecution*. The Privy Council stated that Hearsay can or cannot be used as evidence for a statement made to a witness by someone who is not summoned as a witness. When the goal of the evidence is to prove the veracity of the statement, hearsay is irrelevant and inadmissible. It is not considered hearsay and can be included if evidence is shown to support not the veracity of the statement but rather its making. It should be noted that a contemporaneous recording which may prima facie infringe an exclusionary rule of evidence called

“hearsay” may be admissible by the Evidence (Special Provisions) Act of 1995. (Hereafter called ESPA)

3.5 Probable Problem Before the Judiciary

We are in a world where technology has taken over our lives by expanding to technological flourishing by making our lives easy. Notwithstanding such easiness, the technology may be a great disadvantage in some aspects. Considering the deep-fake technology, as mentioned in the definition, this technology can manipulate the identity of a person in many ways such as manipulation of photographs, manipulation of videos and audio. Through this method, deep-fake technology can become very dangerous for political context, individual rights context under violation of the right to privacy and right to free thoughts, legal and social context.

In this scrutiny, manipulation of audio, video and picture evidence through deep-fake technology has been addressed. The deep-fake arises in two circumstances as evidence in legal proceedings. Number one is as the subject matter of a particular claim and the second instance is to support a different claim. The deep-fake technology uses the same techniques to manipulate videos and photos (Huijstee)—manipulation of photographs started with the popularity of the application Photoshop in the 90s. Unlike the applications like Photoshop, the user/image processor does not have to alter the image manually in deep-fake. Deep-fake technology has developed techniques to alter an image automatically. Automatic image alteration first came to society as early as the '90s through a video rewriter programme that synthesized the facial animation of former United States President John F. Kennedy (Bregler, Covelle and Slaney, 1997). Deep-fake technology can be used to manipulate images, audio and video that would make a person appear authentic and truthful. This is a result of Generative Adversarial Networks (GAN) where two artificial neural networks work and compete to create realistic media (Westerlund, 2019).

The Author of the book “Trust No One: Inside the World of Deepfakes, Michael Grothouse stated that “I tried an armed robbery and it's on video. It was recorded by a GoPro camera positioned on the victim's head. He rode his bike along the street, going about his

business as usual. The video abruptly cuts to me arriving on a motorbike drawing a revolver and making him halt in his tracks. He goes on, "But even though this video purports to show me doing the crime, it never really happened." (Grothaus, 2021)

Disinformation such as that mentioned in the above paragraph can be established in society through deep fakes. There are two (2) methods that deep fakes support disinformation which can mislead the courts. One method is convincing misinformation and the second is supporting misinformation to increase its misleading potential (Mariëtte van Huijstee et al, 2021). In this sense, the ultimate goal of the law, called "justice" would be manipulated. In addition to that standing adversely, a suspect may claim that the evidence against him/ her is false and constructed through deep fake technology. In such cases, despite proving the accused is guilty, the state has to prove the contemporaneous recording evidence against the accused is not altered or tampered with. Not only in criminal cases also in civil cases deep-fakes can be seen. To mitigate misleads in civil or criminal proceedings through deep-fakes under the context of evidence, the probable and practical remedies are mentioned in the very next part of this paper. The solutions are discussed under the contexts of authentication of contemporaneous recording evidence and the penal laws that shall be imposed.

3.6 Sri Lankan Law on Perjury

By reading Section 188, 189 of the Penal Code of 1883 and Section 449 of 1979 Criminal Procedure Code Act and as per the Section 161 of Administration of Justice Law No. 44 of 1973, it is a criminal offence to submit or create false evidence in the Supreme Court, Court of Appeal of High Court which would followed by either simple or rigorous imprisonment not exceeding two (2) years or fine of not exceeding than one thousand (1,000) Sri Lanka Rupees. If the false evidence was submitted to an inferior court, a punishment of either simple or rigorous imprisonment or a fine not exceeding five hundred (500) Sri Lankan Rupees. It is noteworthy that mere conflict of evidence does not raise perjury through false evidence (*Attorney General v. Silvan Silva* [1981 01 SLR 364 / 1981 01 Sri LR 364]), the judicial power to punish perjury

shall be exercised when the judge is clear beyond reasonable doubt as discussed in the case *Vithara v The State* [1992 01 SLR 367 / 1992 01 Sri LR 367].

4. RECOMMENDATIONS AND CONCLUSION

To provide effective guidance on the use of deepfakes, it is crucial to understand the various groups that create them. This includes deep-fake enthusiasts who make them for pornographic, social media, and entertainment purposes, as well as for commercial jobs. Political entities, fraudsters, and legitimate actors like cinematograph makers, television companies, and commercial advertisers also use deepfakes. Recommendations should balance the legitimate uses of deepfakes while also preventing harmful deepfakes that exploit personal data and harm society. Proposed measures include recommendations for innovative authentication systems for audiovisual evidence, registration of legitimate deep-fake makers, a licensing regime for deep-fake software in Sri Lanka, and separate laws to govern the licensing and legitimate use of deep-fakes. Penalties should also be imposed for creating illegitimate deepfakes, regardless of their commercial or non-commercial purposes. Ultimately, the goal is to mitigate the immoral and illegitimate uses of deepfakes that are prohibited by law.

To effectively address the issue of deep fakes, the law must prohibit the intentional creation and distribution of harmful deep fakes that are designed to mislead society, as well as the wrongful use of personal data. Additionally, the distribution of deep fakes with knowledge of their falsity must be prohibited, even if this limits the freedom of expression established by Article 14 (1) (a) of the Sri Lankan Constitution. It is important to note that the freedom of expression is not an absolute right and is limited by Article 15 (2) of the Sri Lankan Constitution in the interest of racial harmony, parliamentary privileges, contempt of courts, defamation, and incitement of offences. Furthermore, it is crucial to recognize that the distribution of tampered audio-visual materials is considered defamation and distributing deep-fake evidence is against common law and can be

considered contempt of courts (Section 449, Code of Criminal Procedure Act No. 15 of 1979). Therefore, a licensing regime should be established for legitimate deep fake creators and distributors. This licensing regime should require the registration of all legitimate deep fake creators and distributors, as well as the watermarking of all legitimate deep fakes. In addition, the watermark of the legitimate deep fake makers should also be registered and the software used by the legitimate deep fake maker should be registered as well. This will make it easier for legal authorities to identify unauthorized and illegitimate deep-fake creation and distribution. It should be noted that non-registered deep-fake makers and software should be prohibited by the proposed legislation, regardless of mens rea (wrongful mind). The defence established by section 72 of Penal Code No 2 of 1883, which reads "Nothing is an offence which is done by any person who is justified by law, or who because of a mistake of fact and not by reason and not by mistake of law in good faith believes himself to be justified by law in doing it," should not apply to non-registered deep-fake creations. This is because deep fakes have the potential to cause significant harm to individuals and society as a whole, and it is, therefore, necessary to regulate their creation and distribution responsibly. In summary, the proposed legislation should focus on prohibiting the creation and distribution of harmful deep fakes that are designed to mislead society, as well as the wrongful use of personal data. A licensing regime should be established for legitimate deep fake creators and distributors, with requirements for registration and watermarking. Non-registered deep-fake makers and software should be prohibited, regardless of mens rea. By implementing these measures, legal authorities will be better equipped to identify and address deep-fake creation and distribution.

It is essential to implement the "Deep-fake Prohibition Law" promptly. This legislation enforces strict liability for non-registration in cases of deep-fake creation. Due to the difficulty in technologically authenticating deep-fakes, strict laws are necessary to prevent their distribution without proper registration. The software used for deep fake creation must be banned from being used and sold in Sri Lanka, except

for those registered correspondingly to the licensing regime. The courts must adopt an accurate authentication method and repeal section 9 of the Evidence (Special Provisions) Act of 1995. This section supports the judiciary to presume the authenticity and accuracy of the contemporaneous recording submitted as evidence. Instead of such presumption or vesting the burden to the opposition to prove the inaccuracy, the judiciary shall adopt an authentication module that can detect deep fakes as well as general alterations done to a piece of audio-visual evidence. Although it is expensive to develop a deep-fake authentication system, the government should invest in this particular field. This is important for public welfare, and security, and as the state policy is to full realization of fundamental rights. The proposed Act criminalises both the illegitimate creation and intentional distribution of such illegitimate creations. However, the legal authorities can detect the illegitimate creators of deepfakes only at the stage of distribution. One of the objectives of Criminal and Penal Laws is to mitigate commissions of offences by imposing laws and penalties thereof. Therefore, it is crucial to make laws on immoral and illegitimate uses of deep-fake to mitigate the tendering of deep-fake audio-visual evidence. The implementation of the law prohibits illegitimate deep-fakes, which helps to mitigate other immoral uses of deep-fakes, such as pornographic content, defamations, and misleadings. To constitute criminal liability on deep-fake, it requires an established criminal and/or penal law to uphold the principle of legality aligned with the rule of law. Although section 449 of the Code of Criminal Procedure Act No. 15 of 1979, section 188 criminalizes submitting false evidence intentionally, and section 189 of the Penal Code criminalizes making false evidence, the mens rea of the creator of deep-fake evidence may not be presented as he/she has not intentionally perjury. Since the deep-fake evidence has been used to mislead the courts by another party without the knowledge of the creator, such a creator will not be criminalized. By imposing laws against the immoral use of deep fakes, we can address directly the root of the misleading. However, it is practically impossible to stop the commission of offences. A strict law will be helpful to reduce the rate of commission of offences.

For another technological method, this paper suggests the relevant authorities to create an artificial intelligence-powered database, which consists of photographs of the faces of all persons who are citizens of Sri Lanka who have got the national identity card. In the national identity card issuing process, the photographs have to be submitted and the database can be filled up with those photographs. The database system shall be powered by artificial intelligence which can identify a similar person by the photo submitted to the database, even in situations where that person is older than when he/she submitted the photo to the database. Highly accurate difference detection algorithms must be fed to the system that can authenticate the visual evidence tendered to the judiciary. A similar process can be facilitated in audio too. To completely stop illegal uses of personal data such as appearance and voice for illegitimate deep-fake creations, the relevant authorities can link the data with the internet to deny uploading or downloading photographs on the internet, which does not give a password or bio-metric recognition authentication. Such passwords and/or authentication methods also shall be put into the suggested database according to the way how illegitimate deep-fake creators cannot download the tampered audio or visual piece.

As we discussed earlier in this paper under the topic of “Shaping the Law to Combat Deep Fake Misleading in Evidence Under the Context of Admissibility of Contemporaneous Recordings as Evidence: Recommendations for Digital Dilemma in the Legal Eye”, deep fake misleading of courts is a probable issue that can arise before us shortly. The presumption in Section 9 of the ESPA 1995, has to be replaced with an alternative section which directs the courts to authenticate any contemporaneous recording that comes before the judiciary as evidence. To create such a directive authority, the local government must facilitate in development of deep fake authentication systems. As a suggestion “hash ID” watermarking system can be recommended. The papers suggest an imposition of criminal offences against illegitimate deep fake creators who are not registered according to the licensing regime suggested by the paper. On the other hand, the readers of this paper shall not

understand that the recommendation is a rejection of contemporaneous recordings as evidence. It is very important to admit audio-visual evidence.

5. REFERENCES

Abu Bakr v. The Queen (1953) 54 NLR 566 (Supreme Court of Ceylon).

Attorney General v. *Silvan Silva* (1981) 1 Sri LR 364 (Supreme Court of Sri Lanka).

Benwell v. Republic of Sri Lanka (1978–1979) 1 Sri LR 194 (Supreme Court of Sri Lanka).

Chalmers, J. (2012) *Evidence Essentials*. Edinburgh: Edinburgh University Press. ISBN 9781845861353.

Christoph, B., Covelle, M. and Slaney, M. (1997) *Video Rewrite: Driving Visual Speech with Audio*. Interval Research Corporation.

Cochran, D., Kelly, M.A. and Gulycz, M. (2016) *Rules of Evidence: A Practical Approach*. 2nd edn. Toronto: Emond Publishing. ISBN 9781772550327.

Debesu, K. and Eshetu, A. (2009) *Law of Evidence: Teaching Material*. Addis Ababa: Justice and Legal System Research Institute. Available at: [teaching material PDF]. (No ISBN; teaching material published under JLSRI sponsorship.)

Dennis, I.H. (2020) *The Law of Evidence*. 7th edn. London: Sweet & Maxwell. ISBN 9780414070946.

European Parliamentary Research Service (2021) *Tackling deepfakes in European policy*. European Parliament. Available at: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA\(2021\)690039](https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)690039)

Grothaus, M. (2021) *Trust No One: Inside the World of Deepfakes*. London: Hodder & Stoughton. ISBN 9781529393169.

Huijstee, M. van (2021) *Tackling Deepfakes in European Policy*. Luxembourg: European Parliamentary Research Service, Scientific Foresight Unit (STOA). Available at:

[https://www.europarl.europa.eu/stoa/en/document/EP_RS_STU\(2021\)690039](https://www.europarl.europa.eu/stoa/en/document/EP_RS_STU(2021)690039)

K.H.M.H. Karunaratne v. The Queen (1967) 69 NLR 10 (Supreme Court of Ceylon).

Kularatne and Another v. Rajapakse (1985) 1 Sri LR 24 (Supreme Court of Sri Lanka).

LaMonaga, J. P. (2020) 'A Break From Reality: Modernizing Authentication Standards for Digital Video Evidence in the Era of Deepfakes', *American University Law Review*, 69(6), pp. 1945–1988. Available at: <https://digitalcommons.wcl.american.edu/aulr/vol69/iss6/5/>

Marine Star (Pvt) Ltd v. Amanda Foods Lanka (Pvt) Ltd (2008) (High Court of the Western Province, exercising civil jurisdiction, Sri Lanka).

Roberts and Another v. Ratnayake and Others (1986) 2 Sri LR 36 (Supreme Court of Sri Lanka).

Ross, M. L., Chalmers, J., Walker, A. G. and Lockhart, W. N. M. (2009) *Walker and Walker: The Law of Evidence in Scotland*. 3rd edn. Haywards Heath: Tottel. ISBN 9781845921651.

Shahul Hameed and Another v. Ranasinghe and Others (1990) 1 Sri LR 104 (Supreme Court of Sri Lanka).

Sri Lanka (1995) *Evidence (Special Provisions) Act*, No. 14 of 1995, s. 6(2). (Enacted: 31 July 1995). Available at: Parliament of Sri Lanka / consolidated statutes.

Subramaniam v. Director of Public Prosecutions [1956] 1 WLR 965 (Privy Council).

Vitharana v. *The State* (1992) 1 Sri LR 367 (Supreme Court of Sri Lanka).

Westerlund, M. (2019) 'The Emergence of Deepfake Technology: A Review', *Technology Innovation Management Review*, 9(11), pp. 39–52. doi: 10.22215/timreview/1282.

Wickremasinghe, S.A. In re (1954) 55 NLR 511 (Supreme Court of Ceylon).