Proceedings of the
36th International Conference on Information Technologies (InfoTech-2022)
IEEE Conference, Rec. # 55606, 15-16 September 2022, Bulgaria

HOW ROBUST IS THE UNITED KINGDOM JUSTICE SYSTEM AGAINST THE ADVANCE OF DEEPFAKE AUDIO AND VIDEO?

Dr Karl O. Jones[1] and Bethan S. Jones[2]

(1) School of Engineering, Liverpool John Moores University, Liverpool
(2) Law School, University of Cumbria, Carlisle, Cumbria
e-mail: k.o.jones@ljmu.ac.uk
United Kingdom

Abstract: A recent development is the application of AI to either alter or create video and audio files - called Deepfakes. The paper examines the issues arising from deepfakes, to determine how robust the UK justice system is against deepfakes. The work analyses deepfake technology, with respect to an evaluation of professional knowledge, evidential standards, and current legislation. The paper discusses difficulties presented by deepfakes, highlighting the need for methods to authenticate digital evidence, and considers what UK legal remedies can protect the justice system and public from digitally falsified evidence. The paper concludes with potential recommendations for the justice system.
Key words: Audio Forensics, Deepfake, Law, Video Forensics.

1. INTRODUCTION

The aim of this work was to determine the robustness of the United Kingdom (UK) justice system against the advances of deepfake audio and video technology [1], by evaluating how equipped the justice system is in handling this new technology.

Deepfakes are defined as 'artificial intelligence or machine-learning applications that merge, combine, replace and superimpose images and video clips onto a video, creating a fake video that appears authentic' [2]. Arguably, knowledge of deepfakes is incredibly uncommon in the justice system; many individuals, government agencies and policy makers misunderstand their importance and possible impact [3], especially regarding the risks they pose to legal and regulatory systems. Remarkably, a lack of findings in legislation, establishes that legal professionals are

unable to protect the public from deepfake technology. Furthermore, it is worthy to note there is a lack of standards and processes governing deepfakes and their presence within the justice system [4]. Worryingly, other legal jurisdictions have a wider grasp and knowledge of deepfakes and are therefore better prepared to handle their existence within the law [1]. Moreover, case law surrounding deepfakes is incredibly sparse with no evidentiary processes being displayed [5]. This paper explores the relationship between audio and video deepfakes, and evidential processes and procedures, resulting in an evaluation of UK Law, leading to suggestions for potential reforms. This area of research is highly significant within the UK justice system because deepfake technology can create serious doubts for the reliability of evidence [5], which creates serious concerns for miscarriages of justice and perverting the course of justice. The paper will deeply challenge the difficulties created by deepfake technology, along with scrutinizing English law to evaluate the difference in protection given to the public against the dangers of deepfake technology [1].

2. AUDIO AND VIDEO DEEPFAKES

In reality, there are numerous examples of deepfakes, many encompassing superimposed images and videos of celebrities [1]. However, the history of deepfakes can be split into two categories; fakes and deepfakes. This is because fakes are created by humans undertaking the work themselves, whereas deepfakes require deep learning processes [6] and are effectively creating something that has never been real [2]. One of the most prominent forms of deepfakes are those related to pornography.

Since deep learning processes focuses on the ability to learn from inputted data [7], it is understandable to see how deepfakes are so easily created, establishing their ever-growing presence in society. One approach to creating a deepfake video requires the developer to train a neural network with many hours of video footage of the person being ‘faked’ so that an understanding of what they look like and how they move is gained. Following this, the trained neural network works with computer generated graphics to superimpose the ‘faked’ person onto a different actor. Similarly, for audio, the neural network uses many hours of audio recordings to learn the person’s voice and inflections, such that it generates an audio file from a written script [7]. One notable deepfake is the video of footballer David Beckham apparently speaking several languages fluently for a “Malaria Must Die” advert [8], an image from the video is shown in Fig 1.

University of Washington researchers created a realistic version of President Barack Obama, including a precise model of how his mouth moves allowing them to make their deepfake Obama ‘say’ anything they wished [9]. Cybersecurity company

Deeptrace™ estimates there were 14,698 deepfake videos online in 2019, up from 7,964 the previous year [10].

Fig. 1 David Beckham deepfake audio and video.

The complexity of deepfake technology [7] allows it to create faces of people that do not exist, such as that shown in Fig. 2. Without suitable procedures in place only obvious flaws in facial generation might be noticed giving a hint at a deepfake image.

Fig. 2 Two images from “thispersondoesnotexist.com”.

A deepfake that has come to light recently is voice cloning [6]. In 2020, a Hong Kong bank manager received a telephone call from a man whose voice he recognized as company a director with whom he had spoken before. This company was about to make an acquisition, and hence required the bank to authorise a transfer of $35 million. Later, it was discovered that the bank manager had been deceived, where fraudsters had utilised deepfake technology to clone the director’s voice [6].

Deepfakes have been presented to a UK court in the form of audio evidence. Byron James, a UK family lawyer, said, '*deepfake audio was used in a custody battle to try and portray a father as threatening*' [3]. Here the deepfake audio was created using freely available systems on the internet '*to create highly sophisticated and plausible fake footage*' [3].

3. KNOWLEDGE OF JUSTICE SYSTEM LEGAL PROFESSIONALS

From the lack of information currently available [11], it is clear that many professionals within the UK justice system are unaware of deepfakes and their scope within society [3]. UK family lawyer Byron James argues, '*courts take evidence such as audio recordings, visual footage and written documents at face value*', when in reality courts should be sceptical, adding, '*the whole legal system needs to catch up, it's not good at technology, there are really easy ways to manipulate the system*' [3].

3.1. Police and Forensic Technicians

It is obvious that video and audio recordings are now an inherent part of everyday life and are key technologies for both the general public and the police service [12]. However, evidence showing police awareness of deepfakes is sparse, arguably suggesting that they are still unaware of deepfakes and associated malicious capabilities [12].

Similar to police officers, forensic technicians are also generally unaware of deepfake technology and its far-reaching capabilities [12]. This is illustrated through the expectations of the qualifications of audio/video forensic technicians, where many UK police forces do not require a degree qualification and frequently do not even expect proven knowledge of audio/video theory. Arguably, forensic technicians need to be fully aware of deepfake technology and its capabilities since audio/video evidence is widely used in criminal proceedings [13], which potentially might have been manipulated or faked.

3.2. Barristers & Lawyers

Having been convicted of murder from enhanced footage from a surveillance tape, Nooner [5] identifies how barristers are totally unaware of potential doctored evidence. It was stated that '*relevant computer-enhanced still prints made from videotape recordings are admissible in evidence when they are verified as reliable representations of images recorded on master videotapes*' [5]. No attempt was made to verify the reliability of the evidence, including the original surveillance tape [5]. Although this case was in the mid-1990s, similar difficulties are still present, namely that technology is speeding ahead of the justice system, especially in relation to the

knowledge of those employed [3]. The lawyer for a father in a child custody case, Byron James stated, '*this was the first instance in around 30 years of legal practice that he had seen such a case of 'deep faking''* [3]. This provides an insight into the lack of knowledge barristers have around deepfakes and their damaging capabilities [3]. However, James also stated, '*unless you're aware of the possibility of something being fake, it's difficult to know*', suggesting barristers should be more aware of deepfake or doctored evidence, to protect the UK justice system from being exploited.

3.3. Judges

One recent case that exemplifies the lack of knowledge judges have surrounding video technology is the Kyle Rittenhouse Trial in the USA [14]. During the trial, a video was zoomed into to see the specified image more clearly [14]. It was argued by Rittenhouse's lawyer that '*using an iPad to zoom in on a video should not be allowed because Apple's AI creates "what it thinks is there, not what necessarily is there"'* [14]. While this case is not about deepfake technology, arguably, most people are familiar with zooming on photographs taken on their mobile phones, thus having a judge not fully aware of what happens when a zoom is used is of some concern [3]. Arguably, legal professionals who understand AI and deep-learning processes [7], will be shocked to learn that the judge '*bought into that possibility and ruled that the jurors were only allowed to view the video in its original size*' [14]. This points towards the lack of knowledge judges have relating to the scope of deepfake technology [14].

4. EVIDENCE IN THE UK LEGAL SYSTEM

'*Evidence is the information with which the matters requiring proof in a trial are proved*' [15]. Munday [16] states, '*the evidence of a fact is that which tends to prove it… something that may satisfy an inquirer of the fact's existence*'. Arguably, in a court of law the principle of evidence is used to determine a belief in something [15], whether it be through physical or verbal evidence, such as blood evidence or witness testimony. Thus, the notion of evidence is an extremely important factor when discussing deepfakes, since it establishes the court's ability to not only detect but handle the possibility of both perverting the course of justice and miscarriages of justice through doctored evidence.

4.1. Audio and video evidence

Examples of audio evidence are ever-present within the justice system [17], whether it be audio on a tape recording, recorded phone conversations or audio

obtained through recorded police interviews [18] Video evidence within the justice system is an ever-growing phenomenon, encapsulating different types of recordings such as from, CCTV, police body cameras, mobile phones, dash cameras and Ring™ doorbells, which might include audio [17]. The presence of such evidence throughout the justice system creates a variety of complex issues [19], highlighting the need for debate around court processes and procedures, and the awareness of legal professionals, of both handling and understanding the physics/technology of this type of evidence, e.g. how a camera lens might distort an image.

4.2. Deepfake evidence

All evidence, whether it be audio, video, blood, fingerprints etc must be handled correctly to avoid corruption [4], as Horsman and Sunde [20] state '*evidence must be reliable if it is to be used as part of any legal decision making*'. Camacho *et al.* [21] state '*an audio recording can be used as evidence in a legal process only if the integrity of the recording is demonstrated… the file has not been manipulated either by the victim, the suspect or by a third part*'. This demonstrates the lack of knowledge and understanding within the justice system relating to possible deepfake evidence since currently, there are no identifiable practices defined either by custom or statute to handle this type of evidence. For example, if the evidence introduced into court was already manipulated prior to seizure by the police [21], this creates serious concerns regarding the fairness of the law [3].

4.3. Audio and video Forensics

The British Standards Institute [4] assert '*an organisation should adopt policies and plans to assure the preservation of digital evidence and… the organisation should maintain processes that assure the integrity of investigations, the independence of experts, and the evidential value of binary information*'. Therefore, it is quite worrying to note that police forces have no processes or procedures in place to establish, maintain or preserve the integrity of digital evidence [22]. The case of Victoria Breeden [17] demonstrates how law authorities are blind to the ever-growing phenomenon of potential deepfake digital evidence [17]. This case involved a recording of Breeden stating '*how easy would it be to make someone disappear*' [17], regarding hiring a hitman to kill her ex-husband. The police took the recording at face value, carrying out no work to determine the authenticity of the recording since it was made by a third party.

This situation creates a serious problem within the justice system, because not only are legal professionals not looking for manipulated evidence, even if they were, they may not notice [4]. As Lv *et al.* state [23], '*digital audio recording is much convenient nowadays… even non-professionals can modify audio without leaving*

any visible traces', for example the free software Audacity (audacityteam.org), is simple to use whilst having powerful audio editing/mixing facilities.

5. UK LEGISLATION

Although legal professionals are aware of fabricated evidence, such as creating fake wills for financial gain, the same individuals have little knowledge of the endless possibilities of deepfake evidence and their impact [3]. One piece of legislation that highlights the issues with deepfake evidence is the Defamation Act 2013 [24]. Section 2, subsection 1 states that '*it is a defence to an action for defamation for the defendant to show that the imputation conveyed by the statement complained of is substantially true*'. If the statement made was manufactured using deepfake technology, the truthfulness of the statement cannot be refuted, since there is no evidence to prove otherwise.

Pavis [25] states, '*the UK is a jurisdiction ripe for reform on the issue of deepfakes as the government is undertaking a series of reviews in connected areas of law*'. Furthermore, '*surprisingly little has been written on deepfakes in relation to UK law*' [25]. Pavis continues, arguing, '*there are significant differences in the legal provisions applicable to Deepfakes between national laws*' [25], indicating that the UK justice system is ill-equipped to handle the advance of deepfake technology, with little to no legislation available to eradicate this digital crime [25].

The Law Commission (TLC) stated that '*as part of its efforts to make the UK the safest place online in the world… the Law Commission was to review the current law around abusive and offensive online communications and highlight any gaps*' [26], as well as reviewing the law on '*online sexual abuse or image-based abuse which included deepfakes*' [25]. However, '*by contrast, Deepfakes were left out of the scope of a subsequent government review assessing the need to reform the UK intellectual property framework in light of AI technology*' [25]. Controversially, TLC did not provide any guidance in tackling deepfake technology [26]. Although there has been acknowledgement of the issues of deepfake technologies within TLC [25], they have not been acted upon.

Instead of reviewing the law once it has been made, contestably, law makers should enable processes to look for deepfakes first, thus eliminating the need for such reviews to take place [25]. This can be done by conducting an investigation into '*how effectively the criminal law protects personal privacy online*' [26], since deepfakes are '*a growing concern in both politics and personal life*' [27].

5.1. Illustrative Example of Problem with Current UK Legislation

While there is no current legislation governing deepfakes [26], existing laws should be kept up to date and fit-for-purpose. The Protection of Children Act 1978

[28], is '*an Act to prevent the exploitation of children by making indecent photographs of them; and to penalise the distribution, showing and advertisement of such indecent photographs*'. Section 7, sub-section 7 states that a '*pseudo-photograph means an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph*'. Furthermore, sub-section 6 identifies that a "child" is '*a person under the age of 18*'. While the term 'pseudo-photograph' accepts an image can be computer generated, debatably, the definition of a 'child' under the Act [28] is a largely contentious issue. If an image has been created through deepfake technology, the individual in the photograph, arguably, does not exist. It is therefore necessary to put forward an argument of whether the image truly depicts a real 'person'. Arguably, the definition of a 'person' is highly subjective, dependent on personal interpretation. Some may only identify a 'person' as anyone with a heartbeat, while others can assume someone is a 'person' simply by viewing an image. Thus, current legislation should keep up to date with new technologies, since if the image was first established to be real or fake, resources, time and money would be spared. Another issue is shown in the wording of section 7, sub-section 7, where the Act relates to a type of image, '*which appears to be a photograph*' [28]. The term '*appears*' creates serious concern, as to be shown as reliable within a court of law, evidence must be authenticated [15]; appearing as something should not be an indication of trustworthiness, especially regarding the ease with which deepfakes are currently being created [29]. Arguably, 'seeing is believing; people tend to accept images 'at face value'' [2]. Due to the probative value attached to images at trial, '*a photograph passes for incontrovertible proof that a given thing happened*' [30], leading people to be susceptible of being misled, because they will be convinced, regardless of whether the videos and images might have been fabricated' [2].

5.2. Improvements

Discussing the need for reform, Hany Farid, Professor at University of California, argues deepfakes are a '*technology that is easily weaponized*' [27], with Siwei Lyu, Professor at University of Albany, adding that deepfakes are a '*problem that isn't going to go away*' [27].

Albert Cahn, Executive Director of the Surveillance Technology Oversight Project, argues, '*laws must be updated to protect against clear cases of digital harassment… but government entities must avoid legislating for or against specific features because the technology is evolving rapidly*' [27]. However, David Greene, notes, '*if a deepfake is used for criminal purposes, then criminal laws will apply. There is no need to make new, specific laws about deepfakes*' [27], suggesting new laws are not essential, rebutting the argument that any improvements are required at all [27].

5.3. Comparison

There is a significant lack of legislation within England and Wales governing deepfake technology [1]. However, it is interesting to note that Scottish Law differs slightly in its response criminalising '*non-consensual disclosure of intimate photographs and films, with both 'photograph' and 'film' defined to include 'whether or not the image has been altered in any way'*' [31]. While it could be argued that Scottish Law targets pornographic manipulated content more specifically [31], other jurisdictions specifically seek out deepfakes [1]. Greengard [27] argues that '*not surprisingly, deepfakes are also testing the legal system and prompting the U.S. Congress, States, and other entities to take action*' [27]. An example of this can be shown quite recently, in September 2019 [1], when '*Texas law… criminalised the creation of a 'deep fake video' and causing it to be published or distributed within 30 days of an election, with intent to injure a candidate or influence an election result*' [1]. Furthermore, the proposed US Malicious Deep Fake Prohibition Act of 2018 '*would introduce penalties for those who create, with intent to distribute, fake videos that facilitate criminal or tortious conduct*' [27].

6. RECOMMENDATIONS FOR IMPROVEMENT

Clearly, the lack of law and the problems existing with current legislation created by deepfake technology plainly shows the need for reform [28]. While deepfakes have been in existence for some years, within the justice system they are in their infancy but are beginning to concern legal scholars. Instead of actually targeting the issue head on to eradicate their use within the courtroom [29], effort has been directed at '*how to prevent, mitigate, and punish the abuse of deepfake technology for harmful purposes*' [29].

6.1. Lack of Professional Knowledge

Pfefferkorn argues '*deepfakes will soon make trial attorneys' and judges' jobs more difficult… they will complicate normal trial proceedings and may give courts reason to revisit the continued adequacy of current rules and standards governing digital evidence*' [29]. Thus, it is imperative that legal professionals become educated about the ever-growing presence deepfakes in the courtroom. Ideally this education should be provided by specialists in audio/video technology, and by specialists in artificial intelligence.

Additionally, forensic technicians must also be trained in correct processing of audio/video evidence in general, as well as in methods for attempting to identify deepfake material.

Furthermore, UK police require training in their approach to seizing audio/video material for evidential purposes, for example currently the technical

specifications of video cameras or audio recording devices are not required to be documented, thus making appropriate forensic processing of the material problematic.

6.2. Standards, Processes and Procedures

Pfefferkorn suggested '*if proving which videos are fake becomes too difficult, then maybe it would be easier to establish which videos aren't…to prove an affirmative rather than a negative*' [29]. However, the same problems would still arise, if no processes and standards exist, there is no way to authenticate evidence [1]. Furthermore, the sophistication of deepfake systems will continue to advance making it harder for people to tell real from fake.

Although the UK justice system has standards and processes regarding the reliability of evidence [32][33], debatably there is an apparent absence of standards and processes addressing deepfake technology [1]. In contrast, standards and processes surrounding deepfakes exist within different legal systems [1]. In detecting deepfakes, '*the U.S. government, academia, nonprofits, and the tech industry have all launched initiatives…to push forward the state of technology for detecting deepfakes*' [29]. Clearly similar initiatives are required for the UK justice system.

6.3. Legislation

Worryingly, if reforms are not taken seriously by legal professionals and policy makers, then there will be severe ramifications from the existence of evidence created/modified through deepfake within the justice system. The challenge of tackling the reliability of digital evidence within the courtroom is an epidemic the UK justice system is ill-equipped to handle [1], something that will only get worse if reforms are not made promptly throughout the judicial system.

7. CLOSING COMMENTS

It is clear to see that the UK justice system is wholly unaware and oblivious to the ever-growing presence of audio/video deepfake technology [1]. The paper has identified that there is a significant absence of legal professional knowledge relating to deepfake technology and its capabilities [3]. This obviously creates a concern regarding the operational procedures of the courtroom [29], since '*lawyers will have to exercise greater diligence in verifying the authenticity of video evidence…that includes learning the signs of a deepfake*' [29]. Furthermore, the paper clearly illustrates that there are no existing evidential standards, processes or procedures to either handle or detect deepfake material [11][33]. Logically then, the justice system cannot be shown to be robust against the advance of deepfake technology.

Debatably, the UK justice system does not have the necessary capacity to put forward the required processes and standards to tackle deepfake technology, because no knowledge has been gained [1]. Furthermore, the deficiency of law around deepfakes attests to the argument that the UK justice system is ill-equipped and unable to cope [29]. Pfefferkorn questions, '*when deepfakes cause harm - whether on a small scale… or large scale, how should the law respond? What existing civil and criminal laws could be invoked to redress those harms?... and what new regulations may be called for?*' [29]. Perhaps it is the case that deepfakes are such an exclusive and unknown marvel that the law will never be able to catch up [29].

However, it is reasonable to suggest that the UK justice system could be identified as robust against deepfake audio and video technology if professional knowledge is improved, new law is brought into force and evidential processes, standards and procedures were developed [29]. Pfefferkorn claims '*with thoughtful advance preparation, trial lawyers and judges will be equipped to handle this new challenge*' [29].

Thus there is an urgent need for the UK Ministry of Justice, as the lead organisation within the justice system, to begin a process of informing people across the justice system about the existence of deepfakes. This is just a initial step, with a need for further intervention in the form of formal education about deepfake creation and its possible impact on evidence, along with the introduction of processes and procedures to ensure that every effort is made to determine if any audio or video evidence has been subject to any form of deepfake technology. It should be noted that certain proof that audio/video evidence is not deepfake might not be possible, however that should not prevent examination to determine if there is an indication of deepfake material.

REFERENCES

[1] Che Ekaratne, S. (**2020**) Manipulated images: a taxonomy. European Intellectual Property Rights, Vol. 42(6), pp. 353-363.

[2] Maras, M-H. and Alexandrou, A. (**2019**). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. International Journal of Evidence & Proof, Vol. 23 (3), pp. 255-262

[3] The Telegraph. (**2020**). '*Doctored audio evidence used to damn father in custody battle'* www.telegraph.co.uk/news/2020/01/31/deepfake-audio-used-custody-battle-lawyer-reveals-doctored-evidence.

[4] British Standard Institution. (**2016**). Information Technology: Governance of digital forensic risk framework. Standards Publication BS EN ISO/IEC 30121:2016.

[5] Nooner v State of Arkansas (**1995**) 907 S.W.2d 677

[6] Cornell University. (**2014**). *Generative Adversarial Networks.* arxiv.org/abs/1406.2661.

[7] IBM. (**2020**). Deep Learning. (2020) www.ibm.com/cloud/learn/deep-learning.

[8] www.youtube.com/watch?v=QiiSAvKJIHo

[9] Suwajanakorn, S., Seitz, S.M. and Kemelmacher-Shlizerman, I, (**2017**). Synthesizing Obama: Learning Lip Sync from Audio. University of Washington.

[10] DeGeurin, M. (**2021**). Kyle Rittenhouse's Lawyers Claim Zooming-In on an iPad Fundamentally Alters a Digital Image. gizmodo.com/kyle-rittenhouse-s-lawyers-claim-zooming-in-on-an-ipad-1848040149.
[11] Forensic Science Regulator, (**2020**). Codes of Practice and Conduct. 2 FSR-C-119 pp. 1-35
[12] MacLennan-Brown, K. and Cohen, N. (**2020**). Digital Imaging and Multimedia Procedure. Defence Science and Technology Laboratory, Vol. 3, pp. 1-45.
[13] The CCTV User Group. (**2022**). *Concerns about how police process CCTV images for the courts*. www.cctvusergroup.com/post/concerns-about-the-processing-of-cctv-images-for-the-courts-by-the-police.
[14] Palmer, S. (**2021**). '*Kyle Rittenhouse's Lawyers Point Out the Obvious*' www.shellypalmer.com/2021/11/kyle-rittenhouses-lawyers-point-out-the-obvious.
[15] Choo A, *Evidence* (**2018**) 5th edn, Oxford University Press.
[16] Munday, R. (**2018**). *Cross and Tapper on Evidence.* 13th edn, Oxford University Press.
[17] BBC News (**2022**) '*Victoria Breeden jailed for trying to get ex-husband murdered*' www.bbc.co.uk/news/uk-england-cambridgeshire-53612107.
[18] Maher, R.C. (**2018**). *Principles of Forensic Audio Analysis*. Springer International Publishing
[19] Pattenden, R. (**2008**). Authenticating "things" in English law: principles for adducing tangible evidence in common law jury trials. International Journal of Evidence & Proof, Vol. 12(4), pp. 273-302
[20] Horsman, G. and Sunde, N. (**2020**). Part 1: The need for peer review in digital forensics. Forensic Science International: Digital Investigation. Vol. 35.
[21] Camacho, S., Ballesteros, D.M and Renza, D. (**2019**) A cloud-oriented integrity verification system for audio forensics. Computers and Electrical Engineering, Vol. 73, pp. 259-267
[22] Tully, G. (**2021**). Forensic Science Regulator Annual Report 2020.
[23] Lv, Z., Hu, Y., Li, C-T. and Liu, B-B. (**2013**). Audio forensic authentication based on MOCC between ENF and reference signals. IEEE China Summit and International Conference on Signal and Information Processing. pp. 427-431.
[24] Defamation Act 2013. (**2013**). www.legislation.gov.uk/asp/2013/26/contents
[25] Pavis, M. (**2021**). Rebalancing our regulatory response to Deepfakes with performers' rights. Convergence: The International Journal of Research into New Media Technologies, Vol. 27(4), pp. 974-998.
[26] Law Commission (**2018**). Abusive and Offensive Online Communications.
[27] Greengard, S. (**2020**). Will Deepfakes Do Deep Damage? Communications of the Association for Computing Machinery, Vol. 63 (1), pp. 1.
[28] Protection of Children Act 1978. (**1978**). legislation.gov.uk/ukpga/1978/37/contents.
[29] Pfefferkorn, R. (**2009**). "Deepfakes" In The Courtroom. Public Interest Law Journal, Vol. 29, pp. 246-276
[30] Sontag, S. (**1977**). In Plato's Cave on Photography. Delta Books, USA.
[31] Abusive Behaviour and Sexual Harm Act (Scotland) 2016. (**2016**). legislation.gov.uk/asp/2016/22/contents.
[32] Criminal Justice Act 2003. (**2003**). www.legislation.gov.uk/ukpga/2003/44/contents.
[33] Police and Criminal Evidence Act 1984. (**1984**). legislation.gov.uk/ukpga/1984/60/contents.