LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 2 | Issue 3

2024

NAVIGATING THE PSYCHOLOGICAL IMPACT AND ENHANCING PREDICTIVE POLICING IN THE ERA OF DEEPFAKES: LEGAL AND TECHNOLOGICAL SOLUTIONS

Beradar Akash[1]

I. ABSTRACT:

In the contemporary digital era, deep fakes and synthetic media have become an issue that has presented new problems to the legal systems worldwide including the IPC. This study outlines deepfakes starting with the technicality of creating deepfake videos, and the manipulation that goes into producing synthetic media. It further seeks to highlight the current legal provisions under the IPC concerning specific sections 354C, 499 & 503 of the IPC. It evaluates the punitive legislation and the outcomes of these provisions in fighting the misuse of deepfakes. The consequences of these findings are relevant since they create a need for an updated legal framework with the use of technology solutions.

Understanding how other countries are approaching deepfakes can be instructive for India's legal frameworks and comparative analysis of international legal approaches therefore holds important lessons for the country. The present study contributes by adding value to knowledge providing a comprehensive understanding of global issues providing sound advice on how India can improve its legal fight against deepfakes. It further examines the law and ethics of criminalizing deepfakes, while trying to prevent harm to people but having to consider the rights to freedom of speech and privacy at the same time. Based on the existing structure of the legislation, proposals for procedural reforms are developed to improve the work of the IPC on cases of crimes related to deepfakes. Prevention of deep fakes is considered by focusing on raising the public's awareness, which would educate society about being victimized by synthetic media manipulation It provides the use of deep fakes with

[1] Student At Christ Academy Institute of Law

real celebrity cases and explains the severe impact on them. Thus, this research calls for an integrated approach to mitigate the troubles of deepfakes.

II. KEYWORDS-

Deepfakes, Psychological Effect, Predictive Policing, Legal Measures and recommendations, Case studies, Technological solutions

III. INTRODUCTION

As the era of social media is gradually progressing, new and viable techniques in technology such as deepfakes and synthetic media have posed significant legal problems to the legal frameworks in every nation including the Indian Penal Code (IPC). Due to the realistic representation, the technology of deepfakes in the creation of fake videos and fake audio poses severe threats to the private sphere, personal reputation, and social trust.

This study tries to address the concern by assessing the failings of the existing legal structure on deep fake and the need for reforms the significance of the research lies in the fact that it attempts to advance the knowledge concerning the interaction of lawful and technological parameters concerning deep fakes when referring to IPC framework as a legal reference. This paper aims to fill the identified gaps by pointing out the weaknesses of the legal framework which are existing and present worldwide tendencies in this sphere, thus, it provides a rationale for why such research is required and needed and how this result can be used to create a legal response. The implications of deep fakes go beyond and raise legal questions on trust, safety, and ethical use of technology as a tool in society.

"*Deepfake is the latest technology danger to our understanding of trust. They destroy the integrity of what we see and hear, and they speak against the truth of what we see and hear.*"

- Hani Farid, UC Berkeley[2]

[2] Jianlin Chen & Zhen Li, *The Psychological Impact and Mitigation of Deepfakes on Victims*, in *Advanced Computational Methods for Knowledge Engineering* 377, 377–390 (2019), available at https://link.springer.com/chapter/10.1007/978-3-030-83734-1_29..

IV. SIGNIFICANCE OF THE STUDY

The importance of this research can be derived from the timeliness in which it was conducted given deepfakes' status as a highly formidable weapon in the realm of misleading content and blackmail. Hence, due to the failure of existing legal structures to adequately address the challenges, there is a need to carry out a comprehensive study that integrates legal, psychological, and technological aspects. Thus, through identifying the psychological effects on the targets and the possibility of using predictive policing, this study will help policymakers, legal authorities, and technology creators to define the proper approaches to prevent the use of deep fake videos

V. PROBLEM STATEMENT

Even now that deepfakes are quite common, the available legal tools under IPC are still inadequate to address the various problems created by the use of such technology. Currently, there are no detailed legal actions, psychological help mechanisms, or preventive methodologies such as of predictive policing to contain and deter the use of deepfakes appropriately.

VI. OBJECTIVES

- To understand the psychological effect of victim impact of deep fake and measures required to help the victims.
- To assess the existing legal measures based on the IPC of India specifically about deepfakes and overcoming its possible drawbacks.
- To examine how the usage of intelligent systems, specifically in regards to predictive policing approach, may help in identifying and preventing deepfake cases.

VII. HYPOTHESIS

- Deepfake victimization has severe psychological consequences and requires a special focus on support services.
- It has been argued that under the current legal regime forged under the IPC

legislation, there is legal redress for deepfakes.

- Intelligent technologies, such as predictive policing, can help the police discover and prevent deepfakes.

VIII. METHODOLOGY USED FOR RESEARCH

The research methodology adopted in this paper is purely doctrinal. Doctrinal research, also known as library-based research, is a distinctive method of conducting legal research that involves the study and analysis of existing legal provisions, case laws, and scholarly works. This methodology is well suited for examining the theoretical and conceptual aspects of law and for providing a systematic exposition of legal doctrines and principles. The secondary source of data relied on sources such as commentaries, articles, and legal digests are also consulted. The selected sources are completely based on the relevance of the research questions and this analysis entails evaluative scrutiny of the provisions in these sources to establish an emerging trend, research deficits, and emerging prospects to the question posed by deep fakes.

IX. RESEARCH QUESTIONS

1. *WHAT ARE THE PSYCHOLOGICAL IMPACTS OF BEING A VICTIM OF DEEPFAKE, AND WHAT STEPS CAN BECOME AVAILABLE FOR SUCH VICTIMS??*

Deepfake is a category of fake media involving AI and machine learning to build algorithms to produce sophisticated fake images/videos or even fake audio. Such technological platforms can tweak the existing media by pasting someone's face on another person's body; changing the forms of expressions or synthesizing voices that seem to belong to the original person and claiming he said or did something which in real life, they never did. Deepfakes use techniques like generative adversarial networks (GANs) to develop material that is rapidly becoming hard to inform from the original media.

A. Legal Provisions related to the IPC 1860

- ***Section 354C*** defines Voyeurism as photographing or filming a private act without the consent of the person involved.

- ***Section 499*** which talks about defamation is an unlawful act done by speaking or writing, or by drawing a picture, which has the result of harming another's reputation, and it can involve deep fake media as well.
- ***Section 503*** threatening to physically harm a person, harm his or her reputation, or damage his or her property. This provision can be met by threatening to harm or intimidate someone by using deepfakes.[3]

B. Information Technology (IT) Act 2000

- ***Section 66E*** criminalizes taking, publishing, or transmitting an image of a person's private parts for a purpose the person can reasonably expect will not be complied with if the circumstances are such as to make it likely that the person's privacy will be violated.
- ***Section 67*** provides for the actual publication for transmission in electronic form of any matter dangerous to the public on the grounds of obscenity. Section 21 of the anti-fake news law which became enforceable on October 1 2020 allows prosecutors to take obscene or sexually explicit deepfakes to court.
- ***Section 67A*** deals with the penalty that entails the person who publishes or transmits material containing sexually explicit acts. It covers deepfakes concerning such content.[4]

X. THE PSYCHOLOGICAL IMPACTS OF DEEP FAKE VICTIMIZATION

Living with deepfake victimization can cause horrific psychological effects on a person. The first major impact can be illustrated in terms of a sexual violation and the subsequent loss of one's persona. Due to such incidents, victims go through anxiety, depression, and even post- traumatic stress disorder (PTSD) due to adjustment to the fact their image or voice can be false and used to tarnish their reputation or cause them humiliation.

[3] Indian Penal Code 1860, Sec 354, 499, 503

[4] Information Technology Act 2000, Sec 66E, 67, 67A

Besides, deepfakes entail severe social and occupational consequences. Deepfake is highly likely to cause injustice to victims since they will be seen as deceiving someone, expelled from social groups, and possibly dismissed from their jobs if the content is particularly negative. Whereas prior sorts of dangers could be avoided, the unknown and unpredictable nature of cyber-attacks allows anybody to become a victim, leading to a loss of trust in digital communications.[5]

XI. CASE STUDIES TO UNDERSTAND

- 16 MAY 2024 Two videos that trended last month depicted top Bollywood actors Ranveer Singh and Aamir Khan endorsing the Congress party. Both reported to the police that these were produced using deep fake technology and that they had not given their consent. Next, on April 29, Prime Minister Modi expressed his apprehensions about using AI to manipulate the speeches of senior leaders of his party, not excluding himself.

  The following day, police detained two people from various parties, the Aam Aadmi Party (AAP) and Congress, related to a fake video of Home Minister Amit Shah.

- 12 MAY 2024 India Today Fact Check discovered that the video circulating and causing people to panic was fake. The story of a doctor being assaulted on stage during his live show is not pinned on any doctor with the name Dr Devi Shetty. The tone of both, the news anchor and the doctor, was changed. This was digitally manipulated by AI[6]

- Recently, actor and model Ranveer Singh reported to the police over a deep fake video where he was portraying to support a particular

[5] Aniket Aryan, *Deepfakes&Indian Law: Safeguarding Against Digital Deception*, SRIRAMs IAS, (Jul 23, 2024, 11.30 AM) https://www.sriramsias.com/upsc-daily-current-affairs/deepfakes-and-legal-provisions-in-india/

[6] Vikas Bhadauria, Fact Check: *This Aaj Tak show about doctor being attacked on air is a DEEPFAKE*, INDIA TODAY, May 12, 2024, (Jul 23, 2024, 11.30 AM) https://www.indiatoday.in/fact-check/story/fact-check-this-aaj-tak-show-about-doctor-being-attacked-on-air-is-a-deepfake-2538184-2024-05-12

political party. Ranveer Singh had already mocked the BJP and Prime Minister Narendra Modi over the problems of inflation and unemployment in a deepfake video.

- Infosys founder Narayana Murthy has said that there are already many fake videos with him on the internet. “That's why there has been a lot of fake news in the previous few months, spread via social media applications and various websites where I have allegedly endorsed or invested in applications for automated trading," Murthy wrote on the Twitter platform.
- The second video which was also misleading showed the actress of Indian origin, Priyanka Chopra, endorsing a brand and stating her annual income. Unlike other actors, Priyanka’s face certainly does not morph in any of the anti-feminist, hate speech, and, or Ethnic Cleansing videos. However, the audio which contains her voice and some lines said in the original video has been replaced by the fake brand advertisement.
- In January 2024, master Indian cricketer Sachin Tendulkar shared on X (ex-Twitter) that a fake video with his face exists on social networks for a certain mobile application. He spoke of his disappointment in how people have opted to misuse different technologies. “These videos are fake.
- parallel They have recently started mimicking ads through a deepfake involving Virat Kohli in one of the digital scams.
- The latest to be a victim of such fraud is Mr. Madhusudan Kela, an eminent investor and Chairman, and Managing Director of MK Ventures.
- Earlier this month on the 5th of December 2023, former chairman of the Tata Group, Ratan Tata, reported a fake video on Instagram in which a look-alike of him gives investment tips. The video was

posted by user Sona Agarwal, and the video was fake, showing Tata as the investment expert providing them investment advice along with the caption letting the users know that they could double their investments risk-free.

- An embarrassing video of the up-and-coming actress Rashmika Mandanna went viral on social media early last November. As a result, the actress without any delay set out a post on her social media handle to articulate her concern.
- The same can be said about an equally specious deepfake video involving a Bollywood actor Alia Bhatt that was also proven to be fake. Sharing the link to the viral video, which superimposes Bhatt's face onto another woman, the latter can be seen posing while resting on a bed.[7]

XII. MEASURES CAN BE IMPLEMENTED TO SUPPORT VICTIMS:

A. LEGAL RECOURSE AND REFORMS

Among the measures, it is necessary to identify the adoption of clear legal regulation that directly regulates crimes using deep fake. It is therefore necessary to provide legislation that can capture the current legal grey areas such as the one under IPC and craft a new one that can capture the creators and distributors of deepfakes. This would include both victim-centered protection measures and punitive ones: Control tactics include prohibiting direct connection between the victim and the perpetrator, as well as restricting access to unlawful Internet sites.

B. PSYCHOLOGICAL SUPPORT SERVICES:

This means additional attention should be paid to the individuals who must reach Mental health services as early as possible. This implies offering them follow-up

[7] "*From Ratan Tata, Sachin Tendulkar to Madusudan Kela: 9 Well-Known Personalities Who Were Victims of Deepfake Videos*, "LIVEMINT" (July 19, 2024, 11.30 AM), https://www.livemint.com/news/india/from-ratan-tata-sachin-tendulkar-to-madusudan-kela-9-well-known-personalities-who-were-victims-of-deepfake-videos-11710307982420.html.

counselling and therapy as a way of helping them deal with the psychological effects of the crimes on victims. In addition, the social networks and volunteers also help to create a conversation to give the victims a chance to comfort each other, and the feeling they are not the only ones[8]

This is inclusive of post-crisis counseling and psychotherapy for further help comprising of particular problems like fear, sadness, and trauma. There is a need for support groups because the victims can always discuss their experiences with other victims hence, they do not feel lonely. Emergency services should be offered as soon as possible in a state of crisis. Cognitive sessions are also useful in assisting victims respond to emotions and feelings; other services involve referring clients to other professionals. It is also a significant requirement for social networks and volunteers to intervene and contribute to providing the victim psychological support and opening a conversation about the incident to help him or her to stop feeling helpless.

C. TECHNOLOGICAL SOLUTIONS FOR DETECTION AND PREVENTION:

In addition, it is possible to develop further and organize other more effective AI instruments for detecting and fighting fake tools and materials that would further reduce the existence of such hazardous media. These can be helpful, for example, to identify deep fakes immediately and ensure they are not going to create a range of negative effects. There must be harmony between the public and the private institutions since they are the primary agents involved in the introduction of novelty on the market and by the use of proper technologies.[9]

D. PUBLIC AWARENESS CAMPAIGNS:

The awareness of people especially deepfakes and the threats posed by them is also crucial as well. Teaching the public how not to become victims of deepfakes and what steps should be taken if one has to face such an issue will reduce the number of people

[8] Ingrid A. Y. Cheong & J. L. F. Ramirez, *Methods for Enhancing the Security of Deep Learning Systems*, in *Security and Privacy in Deep Learning* 447, 448 (John R. Smith & Lisa B. Johnson eds., Springer 2021), https://link.springer.com/chapter/10.1007/978-3-030-83734-1_29.

[9] Charlotte Bowyer, *The psychology of deepfakes: why we fall for them*, ONFIDO (2023), (Jul 23, 2024, 11.30 AM). https://onfido.com/blog/the-psychology-of-deepfakes-why-we-fall-for-them/.

who are likely to be influenced and will demoralize those negative deepfake interferences. Another need for awareness campaigns is the dissemination of information on the resulting psychological consequences for the victims and the appeal for compassion and acceptance[10]

2. *HOW USEFUL ARE THE EXISTING LAWS BASED ON THE IPC IN TACKLING THE DISCUSSED DEEPFAKE?*

Regarding the current legislation reflected in provisions of the Indian Penal Code (IPC) as far as meeting deepfake challenges, the legal solutions are still in their evolutionary stage. Even in instances where deep fake pornography is involved, the current laws including Section 499 (criminal defamation), Section 500 (punishment for defamation), and Section 503 (criminal intimidation) can be used to explain the factual situations by their very nature of deep fake creates fictitious situations that portray innocent citizens in evil ways and as a result, their reputation and image is attacked and threatened. However, many of these provisions are vague concerning digital environments and the problems posed by deep fakes.

Besides, there is the Information Technology Act of 2000 which works in parallel with the IPC focusing on identity theft, invasion of privacy, and the publication of obscene material. For instance, Section 66E makes it criminal to breach the privacy of an individual, which may come into play when a deepfake violates an individual physical space and or image. Next, Sections 67 and 67A relate to obscene and sexually explicit materials in this regard, despite the inclusion of the above-stated provisions there is a critical gap in the laws as far as handling deep fakes given its potential of having an ill motive as well as the ever-increasing advancement in technology.

E. Addressing the Specific Gaps and Loopholes

i. The IPC and IT Act don't provide enforcement measures for deep fakes explicitly, which results in problems that arise out of attempting to apply old laws to new technologies. Some

[10] Asher Flynn et al., *Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse*, 62 THE BRITISH JOURNAL OF CRIMINOLOGY 1341 (2021), (JULY 23, 2024, 11.30 AM)https://academic.oup.com/bjc/article-abstract/62/6/1341/6448791.

modernistic technologies require separate definitions and provisions that address the issue of their possible misuse.

ii. Deepfakes as deeply integrated into society today outcompete the existing laws due to progress. Current laws can be insufficient to consider new approaches and elaborate techniques followed in making deepfakes.

iii. Although the legal measures that have been provided under the IPC and the IT Act should suffice to cover all the possible depredations of deepfakes, such as the psychological trauma on the victims or misinformation that may be created by the technology, it may not be entirely adequate.

Current debates in the judiciary such as a PIL in Delhi High Court also underline the necessity of proper regulatory measures for AI and deep fake technologies Furthermore, the Indian government is thinking about new IT rules concerning deepfake content moderation, illustrating an active attitude toward the problem. Though there are existing laws provided under the IPC and IT Act, these are still largely inadequate and need improvement to meet the demands of the deep fake content. Thus, it will become imperative for legal standards to evolve progressively as a way of countering technological changes needed to safeguard individuals' rights in the new environment.

XIII. COUNTRIES ABOUT DEEP FAKE LEGISLATION

A. United States

The strategies of the United States concerning deep fakes primarily stem from its United States laws as well as the new proposed legislation. The DEEPFAKES Accountability Act is one such draft bill designed to name deepfakes explicitly. Also, different state laws regulate some aspects of deepfake manipulation, primarily related to interference in the elections and non-consensual erotica. Two of the states of the USA, namely California and Texas, have developed their statutes concerning malicious deepfakes.

B. Britain

The UK mainly deals with deepfakes using data protection and privacy laws. Some measure of protection is provided against the malicious use of personal data in deepfakes from the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). The UK government is also discussing more particular steps to deep fake production and distributing[11]

C. China

China has one of the most elaborate legal systems concerning deepfakes. The Cyberspace Administration of China has issued rules that state that deepfakes must be marked and must not be used for fraudulent, slanderous, or any other unlawful purposes. These regulations preserve the rather vague concepts of privacy, national security, and social stability - which is characteristic of China's overall approach toward much more stringent regulation of digital content.[12]

D. Russia

Russia is comparatively passive in passing legislation that specifically addresses deep fakes; however, it prosecutes deepfakes per its anti-misinformation and cybercrime laws. Thus, deepfakes can be a subject of content regulation by the Russian government together with fake news and other content that violates public order. However, the specific law related to deep fakes is in the development process.

3Q HOW CAN AI-POWERED PREDICTIVE POLICING TOOLS BE UTILIZED TO PREEMPTIVELY IDENTIFY AND MITIGATE DEEPFAKE THREATS?

Technologies like artificial intelligence (AI) and machine learning (ML) have enormous potential for use in the majority of police operations, including the battle against deepfakes. Here's how AI-powered predictive policing tools can be leveraged

[11] *UK Considering Deepfakes from a Data Protection Perspective*, DATA GUIDANCE (July 19, 2024,11.30AM), https://www.dataguidance.com/opinion/uk-considering-deepfakes-data-protection-perspective.

[12] Afiq Fitri, *China has just implemented one of the world's strictest laws on deepfakes*, TECH MONITOR, January 10, 2023, (Jul 23, 2024, 11.30 AM), https://techmonitor.ai/technology/emerging-technology/china-is-about-to-pass-the-worlds-most-comprehensive-law-on-deepfakes.

effectively: From the preceding analysis, it is now possible to highlight the following recommendations concerning the use of AI in predictive policing

Through data analysis, AI can process and extract information from the available big data in real time that may be associated with deepfake production and dissemination. Departments like NYPD and LAPD have tried to integrate technologies into predictive policing to supplement actual time crime examination. Such systems can include such features as to sort out the hot spots of the potential generation and distribution of deepfakes for further actions.

AI algorithms are a perfect tool to find patterns in the data that would be hardly noticed by human analysts. In this way, with the help of training such algorithms on known deepfake datasets, the police can create systems that highlight the corresponding activities or content. This will involve identifying abnormal digital patterns or the fast sharing of content with deep fake elements on multiple social networks

AI could analyze and make decisions based on the large volume of data that may be linked to deepfake generation and distribution in real time. Specific types of data that can be analyzed include:

- Use any social media platforms for posts and shares in the target social media sites such as Facebook, Twitter, and Reddit to see if there is any evidence of deep fake or if there is any noticeable pattern in its usage.
- Checking of the other related meta-data that may come along or is appended to digital files for signs of distortion or manipulation essentially suggestive of deepfake manufacture.
- Image and Video Content: Using artificial smart learning-based systems to visually search for symptoms of alteration or manipulation in the images.

Deepfake detection can be done using different techniques such as Digital Fingerprinting, Audio Anomaly Detection, Video Anomaly Detection, and others. For example, techniques can be created to search videos and Voice-over IP (VoIP) calls for signs of tampering for the authorities to detect deep fakes before they are weaponized.

There is various software that use AI and can be of help to the investigations of such crimes by helping in the collection of digital evidence. This consists of determining the sources of deepfakes, and the nature of distribution channels and connecting them to the culprits using big data analysis and machine learning.

Therefore, using predictive modeling, the AI tools can identify when new deepfake threats are likely to rise based on the trends and previous occurrences. This helps in the replenishment of assets to give priority to areas or people most likely to be affected or engage in deepfake content. Similarly, again, AI can be used to create educational content that would help raise awareness of the general population concerning the dangers of deepfakes and how to detect them.

Although there are solutions to the implementation of AI-powered predictive Policing the danger in algorithm bias, and the problems of surveillance cannot be overlooked. That is why the constant improvement of AI technologies and cooperation with technologists are crucial for countering the threats of deep fakes.

XIV. CONCLUSION & SOLUTIONS

I want to underline that by utilizing these technological solutions, we can reduce the psychological effect of deep fakes and improve predictive policing, thus, creating better conditions for enhancing the level of trust in the digital world.

- Create new and advanced formats of machine learning able to detect fakes by comparing inconsistencies in the source, sound, and vision.
- Introduce the use of blockchain technology that provides a way of generating decentralized, authentic, and tamper-proof records of the original contents.
- Watermark the videos and images that are integrated into videos to make them invisible but noticeable by software utilities for checking media genuineness.
- Mention should also be made of the fact that metadata that is used to track the source of the digital media and any subsequent alteration should be strong.

- Creating public awareness through campaigns that educate the public on the existence of deepfakes, their risks, and what to do in their presence.
- Enshrine into laws that service providers in the digital sphere must incorporate deepfake detection technology and ensure that the manipulated contents are adequately labeled.
- Set legal frameworks regarding accountability of deepfake misuse to have measures in place on the creation and/or dissemination of more nefarious deepfake materials.

Thus, it is crucial to understand that to combat ever-growing deepfakes' problems, a multifaceted solution is needed. This paper is aimed at exposing the existing deficiencies of the IPC and considering the potential changes by learning from the legal systems of the world. The consent is followed by the necessity of psychological services that are needed to provide victims with counseling and therapy due to the severe psychological consequences.

Deepfakes can be recognized and prevented in real-time with the help of technological tools such as AI and machine learning. Other preventive measures include public awareness to enable members of society to identify deep fakes and what ought to be done

In conclusion, it is crucial to employ a multifaceted approach based on legal changes, psychological assistance, and information and communication technologies to address the deepfake problem and secure people's rights in the digital environment.

However, it should be noted that the realization of these solutions presents several Challenges. Hence, the ability to create and sustain sophisticated algorithms incorporating machine learning and blockchain is expensive and might meet opposition owing to its high costs. Watermarking and metadata tracking is as yet in its infancy and requires wider dissemination and still lacks the universal support of common institutionalization. That means that public awareness type of campaigns has to efficiently target various groups of people. Using deep fake detection in-laws may take ages due to the legislation being a slow process or may receive resistance from service providers due to added regulatory measures. Last, to address the misuse of deepfakes, societies need time and new laws that should be established to counter new technologies.

XV. REFERENCES

A. Legislations referred:

- Indian Penal Code 1860, Sec 354, 499, 503
- Information Technology Act 2000, Sec 66E, 67, 67A

B. Others References:

- Jianlin Chen & Zhen Li, *The Psychological Impact and Mitigation of Deepfakes on Victims*, in *Advanced Computational Methods for Knowledge Engineering* 377, 377–390 (2019), available at https://link.springer.com/chapter/10.1007/978-3-030-83734-1_29
- Aniket Aryan, *Deepfakes&Indian Law: Safeguarding Against Digital Deception*, SRIRAMs IAS, (Jul 23, 2024, 11.30 AM) https://www.sriramsias.com/upsc-daily-current-affairs/deepfakes-and-legal-provisions-in-india/
- Vikas Bhadauria, Fact Check: *This Aaj Tak show about a Doctor being attacked on air is a DEEPFAKE*, INDIA TODAY, May 12, 2024, (Jul 23, 2024, 11.30 AM) https://www.indiatoday.in/fact-check/story/fact-check-this-aaj-tak-show-about-doctor-being-attacked-on-air-is-a-deepfake-2538184-2024-05-12
- "*From Ratan Tata, Sachin Tendulkar to Madusudan Kela: 9 Well-Known Personalities Who Were Victims of Deepfake Videos*, "LIVEMINT" (July 19, 2024, 11.30 AM), https://www.livemint.com/news/india/from-ratan-tata-sachin-tendulkar-to-madusudan-kela-9-well-known-personalities-who-were-victims-of-deepfake-videos-11710307982420.html.
- Ingrid A. Y. Cheong & J. L. F. Ramirez, *Methods for Enhancing the Security of Deep Learning Systems*, in *Security and Privacy in Deep Learning* 447, 448 (John R. Smith & Lisa B. Johnson eds., Springer 2021), https://link.springer.com/chapter/10.1007/978-3-030-83734-1_29.
- Charlotte Bowyer, *The psychology of deepfakes: why we fall for them*, ONFIDO (2023), (Jul 23, 2024, 11.30 AM). https://onfido.com/blog/the-psychology-of-deepfakes-why-we-fall-for-them/.
- Asher Flynn et al., *Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country*

Exploration of an Emerging form of Image-Based Sexual Abuse, 62 THE BRITISH JOURNAL OF CRIMINOLOGY 1341 (2021), (JULY 23, 2024, 11.30 AM)https://academic.oup.com/bjc/article-abstract/62/6/1341/6448791

- *UK Considering Deepfakes from a Data Protection Perspective*, DATA GUIDANCE (July 19, 2024,11.30AM)https://www.dataguidance.com/opinion/uk-considering-deepfakes-data-protection-perspective.
- Afiq Fitri, *China has just implemented one of the world's strictest laws on deepfakes*, TECH MONITOR, January 10, 2023, (Jul 23, 2024, 11.30 AM), https://techmonitor.ai/technology/emerging-technology/china-is-about-to-pass-the-worlds-most-comprehensive-law-on-deepfakes.