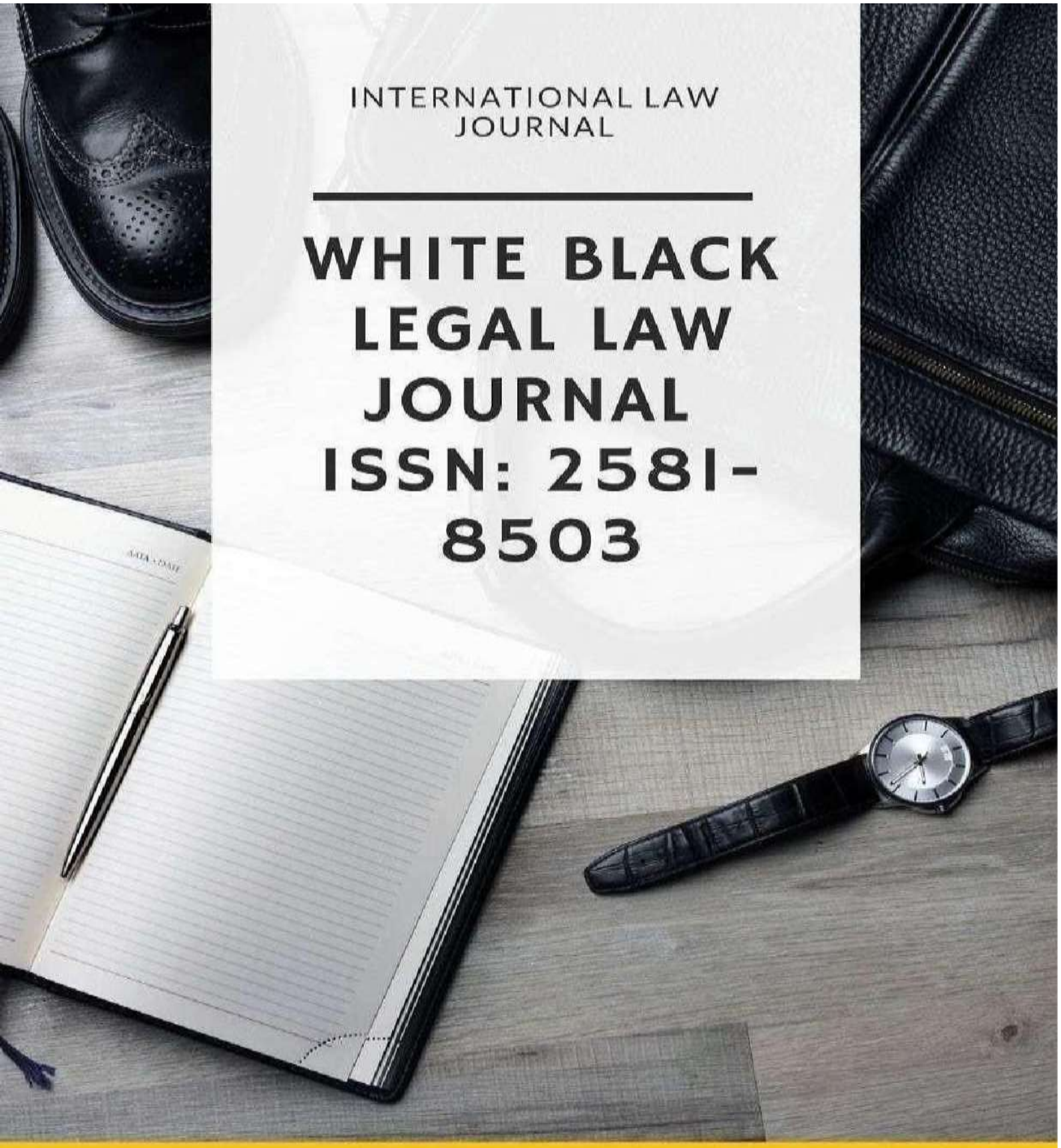

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

DEEPFAKE - A SEVERE FORM OF IDENTITY THEFT

AUTHORED BY - MEHAKPREET KAUR[1]

In digital age, your identity is like your shadow – easy to lose and difficult to reclaim once it's stolen. Dave Marinaccio[2]

INTRODUCTION

Hollywood has glorified hackers. One could imagine multi-million dollar heists where enormous amounts of money are forcibly extracted from banks. But, truth be told, criminals who use the World Wide Web to steal data and money are just like burglars scoping out a home: it's all about easy targets. No matter how careful one may be with the information, there will always be someone crafty enough to come after it in the hopes of selling it or using it to scam you out of your money.[3]

The identity of a person is the most important commodity that a person owns. It is used to prove who we are, where we live and what credit rating we have. This information is a necessary and fundamental part of our everyday modern life. Unfortunately, it can be easily stolen, forged or altered to create a false identity or to steal an existing one.[4] This unlawful use of another person's identifying information is known as identity theft. Identity theft is one of the most feared and fastest-growing crimes which is dangerous for individuals as well as society.[5]

The term 'Identity Theft' comes from a combination of two words Identity and Theft. *Identity* can be defined as the distinguishing character or personality of an individual while *Theft* is

---

[1] Research Scholar, Department of Laws, Guru Nanak Dev University, Amritsar.
[2] An author and advertising executive.
[3] COVE, "Wise Words of Warning: Personal Safety, Freedom, and Security Quotes of the Past," retrieved from <https://www.covesmart.com/resources/home-safety/wise-words-of-warning-personal-safety-freedom-and-security- quotes-of-the-past/> visited on 27.5.2024 at 10:12 pm.
[4] Matthew Record. *Protecting Your Identity: A Practical Guide to Preventing Identity Theft and Its Damaging Consequences* (United Kingdom: How To Books Ltd., 2008) 2.
[5] Nisha Dhanraj Dewani, Zubair Ahmed Khan. (eds.), etal., *Handbook of Research on Cyber Law, Data Protection, and Privacy* (USA: IGI Global, 2022) 37.

defined as the act of stealing; specifically the felonious taking and removing of personal property with intent to deprive the rightful owner of it. Identity theft involves stealing of another person's personal identifying information such as social security number, date of birth and mother's maiden name, and then using the information to fraudulently establish credit, run up debt or take over existing financial accounts.[6] "*If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees."*[7] This is so true and exactly applicable to our lives in this era of the internet.

We live in a dangerous world and in a dangerous time, where evil men would come to steal information and infringe our privacy by committing Identity Theft. Deepfake technology has taken it to more alarming levels by creating fake videos and audio recordings of individuals. It is said that a camera cannot lie. However, in this digital era, it has become abundantly clear that it doesn't necessarily depict the truth. Increasingly sophisticated machine learning and artificial intelligence with inexpensive, easy to use and easily accessible video editing software are allowing more and more people to indulge in generating so-called deep fake videos, photos and audios. These clips, which feature fabricated, altered and fake footage of people and things, are a growing concern in human society.[8]

The deepfake applications appeared in November 2019, but users swiftly amplified it by 100% during the recent COVID-19 pandemic.[9] and India has become the topmost destination for deepfake attacks. Deepfakes are "*a very important, clear and present danger*" to Indian internet users, said Union minister Rajeev Chandrasekhar.[10]

MEANING OF DEEPFAKE

Deepfake is a hyper-realistic media that falsely depict events that never occurred. Deepfake technology combines the words "deep learning" and "fake,". Deepfake uses a kind of artificial

[6] Mahmood Hussain Shah, Paul Jones. (*eds.), etal., Information Technology and People- Cybercrimes prevention: promising organisational practices* (Bingley, UK: Emarald Publishing, 2019) 1185.
[7] Kahlil Gibran, Lebanese-American writer and poet.
[8] Soumya Gangele, "Deepfake: A New Menace," retrieved from <*https://www.cyberpeace.org/resources/blogs/ deepfake-a-new-menace*> visited on 16.12. 2023 at 4:50 pm.
[9] Fakhar Abbas and Araz Taeihagh, "Unmasking deepfakes: A systematic review of deepfake detection and generation techniques using artificial intelligence," *Elsevier Journal* (May 2024) 1.
[10] Smriti Kak Ramachandran, ''PM raises concerns over tech misuse, deepfakes" retrieved from <*https://www.hindustantimes.com/india-news/pm-raises-concerns-over-tech-misuse-deepfakes-101700243985478-amp.html*> visited on 19.11. 2023 at 3:30 pm.

intelligence that is called "deep learning" to fabricate or alter images of fake evens, and hence the name as deepfake. The deepfakes are the synthetic media used to create hoax videos, images and audios which are convincing enough to be believed as real. In simple words, deepfakes are any sort of videos or audios or images of any person that has been altered in a way that they appear to be of someone else and are often used with malicious intention.

Deepfake technology's main goal is to create very realistic synthetic content that looks like actual people, but with some aspects changed. These clips, which feature fabricated, altered and fake footage of people and things, are a growing concern in human society. It has a wide range of applications, including in education to generate interactive content, in the film industry to replace a lead actor with their stunt double or synchronised dubbing for foreign language films, and in the retail sector to improve the overall experience for potential buyers.[11]

Images created using deepfakes technology aren't your average hoax. False visuals of Donald Trump's arrest that went viral before his indictment were created by AI, but they are not deepfakes. Similarly, an AI-generated Pope wearing a puffer jacket does not constitute a deepfake. A deepfake may be distinguished by the presence of human intervention.[12]

Deepfakes are computer trickery that can be used to mimic statements or videos of prominent personalities. Thus, it's a serious issue since it has the potential to spread instability and make it difficult for the public to understand the true nature of politics. Deepfake technology has the potential to generate totally new characters or bring stars back to life for posthumous roles in the entertainment industry. It gets harder and harder to tell fake content from authentic content, which makes it simpler for hackers to trick people and businesses.[13] Its impact in the Indian society is also increasing day by day. Apps like DeepNude allow users to create realistic naked image of women just by uploading an image. Often, the targets are celebrities or people with

---

[11] Ayush Prakash, "How to navigate the web of deepfakes," retrieved from <*https://www-deccanherald-com.cdn.ampproject.org/v/s/www.deccanherald.com/amp/story/opinion%2Fhow-to-nav igate-the-web-of-deepfakes-2808302?amp_gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#amp_tf=From%20%251%24s&aoh=17027348441985&referrer=https%3A%2F%2Fwww.google.com&ampshare=https% 3A%2F%2Fwww.deccanherald.com%2Fopinion%2Fhow-to-navigate-the-web-of-deepfakes-2808302*> visited 25. 01. 2023 at 10:50 pm.

[12] Aditya Mehrotra, "Dissecting the Framework of Deep Fakes in India – A Glaring Lacuna," retrieved from <*https://clt.nliu.ac.in/?p=887*> visited on 15.4.2024 at 3:44 pm.

[13] Soumya Gangele, "Deepfake: A New Menace," retrieved from <*https://www.cyberpeace.org/resources/blogs/de epfake-a-new-menace*> visited on 16.12. 2023 at 4:50 pm.

distinct public image. But there have been instances where the general public has been targeted as information from social media, which lacks privacy settings, are easy to obtain. One cannot wait for the risk imposed by this technology to reach an alarming level.[14]

Deepfake v/s Morphing

Deepfake is a method of digitally altering an image, video, audio or other forms of media. But, so is morphing. The difference comes in the algorithms used for the transformation and the purpose of such an act. Deepfakes use deep learning, in which a computer is trained with a heavy amount of data to do human-like tasks. Morphing, on the other hand, does not rely on AI. It is often used in movies, music videos, and other forms of entertainment to create a transformation effect. Morphing uses a straightforward technique, blending two images to create another image with simple software. For creating deepfake, the technology used is more sophisticated and produces content with a high degree of realism. Deepfakes can be extremely convincing and difficult to detect, sometimes requiring expert analysis or specialised detection software. Morphs are usually easier to spot and often intended to be noticeable as part of a creative effect. As a result, deepfakes are often used with manipulative intent, while morphing is mostly used for entertainment purposes.[15]

TYPES OF DEEPFAKE

Deepfakes can be broadly divided into four categories based on the method of creation employed, namely –

a) Image deepfake which employs the method of face and body swapping;
b) Audio deepfake which employs text-to-speak and voice swapping methods;
c) Video deepfake which employs face-morphing and face-swapping methods; and
d) Audio-visual deepfake which employs lip-syncing in addition to the above methods.

---

[14] Rashi Choudhary, "The Emergence Of Deepfakes In India," retrieved from <*https://thegclsblog.wordpress.com/2020/06/26/the-emergence-of-deepfakes-in-india/*> visited on 16.12. 2023 at 5:50 pm.

[15] Cris, "Explainer: How deepfakes differ from morphing," retrieved from <*https://www-thenewsminute-com.cdn.ampproject.org/v/s/www.thenewsminute.com/amp/story/news/explainer-how-deepfakes-differ-from-morphing?amp_gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#amp_tf=From%20%251%24s&aoh=17159677490324&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.thenewsminute.com%2Fnews%2Fexplainer-how-deepfakes-differ-from-morphing*> visited on 22.05.2024 at 5:45 pm.

PRODUCERS OF DEEPFAKE

Deepfakes are generally produced by different people depending on different motives/ objectives. These include-

1) **Deepfake hobbyists-** Deepfake hobbyists are difficult to track down, they generally are up with swapping up faces of any normal person or celebrities' on bodies of porn stars', followed by making videos like politicians say funny things, destroying one's marriage with an unreal sex video of either of the spouses, or derange an election by releasing a fake or unreal video or audio recording of the candidates days before voting starts. [16]
2) **Political players-** Political players includes the candidates, hackers, terrorists, and foreign states can use deepfakes in spreading fake political information, broadcast fake campaigns to manipulate public opinion and weaken the confidence of people in their country's institutions and its democracy.
3) **Fraudsters-** Fraudsters use for the purpose of stock manipulation and other such financial crimes. They are already using AI generated fake audios to impersonate bank executives on the phone asking for bank card details, OTPs related to bank accounts and sudden cash transfers. In near future, artificial super intelligence would also be capable of faking live video calls and causing more damage to human lives.[17]
4) **Entertainment Companies-** Deepfake technologies are used by several game developers to give face to the game characters and music videos and movie scenes. These are used with the sole purpose of encouraging and showcasing the art of movie making.

WORKING OF DEEPFAKE TECHNOLOGY

Before the emergence of deep fake technology, forgery is usually achieved through the splicing of videos and images. The process of splicing is also a process of covering, by removing, duplicating, shifting, or deleting to achieve the covering and splicing of certain objects. Unlike

[16] Shashank Shekhar and Ashish Ransom, "Ethical & Legal Implications of Deep Fake Technology: A Global Overview," *The Ciencia & Engenharia- Science & Engineering Journal*, Vol. 11, No. 1 (2023) 2227.
[17] *Ibid.*

the splicing of the images and videos, deepfake technology originated from Artificial Neural Network, which is one of the representative algorithms of Deep Learning.

Initial video image forgery mainly depends on the Auto-encoder Network. Autoencoder is an artificial neural network architecture divided into two parts: encoder and decoder. The encoder encodes and compresses face images by extracting the face features, transforming the image into vector values in the latent space, while the decoder reconstructs the original face according to the face features extracted by the encoder, making the data as close as possible to the input data of the encoder.[18] Deepfake technology is based on two techniques, namely, Deep Learning and Generative Adversarial Networks.[19]

USES OF DEEPFAKE

Deepfakes are used for various purposes, both benign and malicious, inter alia, the following:

Postive Uses

Deepfake technology has positive uses in many industries, including-

a. **Film Industry**- The film industry can benefit from deepfake technology as movie makers will be able to recreate classic scenes in movies, create new movies starring long-dead actors, make use of special effects and advanced face editing in post-production, and improve amateur videos to professional quality. Paul Walker, who died before the completion of the movie "Furious 7". Deepfake technology was used to recreate his face for the last scene of the movie.

[18] Min Liu and Xijin Zhang. *Proceedings of the 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022)* (Switzerland: Springer, 2023) 1308.

[19] Shubham Pandey and Gaurav Jadhav, "Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India," retrieved from *<https://www-scconline-com.cdn.ampproject.org/v/s/www.scconline.com/blog/post/2023/03/17/emerging-technologi es-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/amp/?amp_gsa=1&amp_js_v=a9&usqp= mq331AQIUAKwA SCA AgM%3D#amp_tf=From%20%251%24s&aoh=17027344061171&referrer=https%3A%2F%2Fwww.google.com &a mpshare=https%3A%2F%2Fwww.scconline.com%2Fblog%2Fpost%2F2023%2F03%2F17%2Femerging-techno logies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india%2>* visited on 16.12.2023 at 10:12 pm.

b. **Gaming Industry**- Deepfake can also be used in the gaming industry to improve the player's experience. For example, it can be used to develop realistic virtual environments and natural-sounding in-game assistants which improve the user experience.

c. **Social good and medical applications**- Similarly, the technology can have positive uses in the social and medical fields. Deepfakes can help people deal with the loss of loved ones by digitally bringing a deceased friend "back to life", and thereby potentially aiding a grieving loved one to say goodbye to her. Researchers are also exploring the use of GANs to detect abnormalities in X-rays and their potential to detect early signs of diseases. This will assist medical professionals in the early detection of illnesses and potentially save more lives. Further, it can digitally recreate an amputee's limb or allow transgender people to better see themselves as a preferred gender.

d. **Businesses**- For businesses, opportunities include new forms of marketing campaigns, including virtual brand ambassadors, developing cost-effective and accessible learning environments and content, designing and deploying AI-based solutions to detect and counter deepfakes, and, ultimately, developing new offerings and business models supported by deepfakes.

e. **Education sector**- One could also benefit from Deepfake technology, by presenting students with information in compelling ways. For example, being used to recreate historical figures and events to improve student participation in history lessons.[20]

f. **Fashion Industry**- The fashion industry is using deep learning to create new design patterns. Deepfakes carry the potential to enhance the digital customer experience. Deepfakes may be used to create highly tailored material that transforms people into models, allowing them to virtually try on an outfit before purchasing it. For eg.- 'Lenskart' has developed an AI engine that helps achieve these purposes and automatically generates virtual models for advertising and fashion.

[20] Rashi Choudhary, "The Emergence Of Deepfakes In India," retrieved from <*https://thegclsblog.wordpress.com/2020/06/26/the-emergence-of-deepfakes-in-india/*> visited on 16.12. 2023 at 5:50 pm.

Negative uses

The origin of this technology wasn't for any malicious reason. It was to aid the creation of cinematic film footage after an actor died while the cinematic project was still in progress. But it soon turned out to be a menace. It's negative uses include the following-

a. Pornography- The most common use of deepfakes is for non-consensual pornographic content. Faces of female celebrities or ordinary women are swapped onto porn stars' bodies without consent. This violates privacy and causes reputational damage. For instance, an Indian man was arrested in 2019 for making deepfake porn of his girlfriend.[21]
b. Disinformation in Politics- Deepfakes can spread misinformation and propaganda during elections. If unchecked, political deepfakes could undermine free and fair elections. Deepfakes can be used to manipulate political discourse, create fake speeches, or alter the statements of public figures.[22] Perpetrators can use deepfakes to spread false information, manipulate public opinion, or damage the reputation of individuals or organizations.
c. Humor/Parody- Many satirical deepfake videos feature celebrities or politicians. Their face/voice is used in comedic or absurdist situations. While parodying public figures is legal, consent issues arise if private individuals become subjects. Further, humorous fakes can numb audiences to more dangerous uses of this technology.
d. Fraud- AI voice cloning can imitate CEOs or officials to obtain sensitive data. In 2019, this tactic drained €200,000 from a UK energy firm. Deepfakes may also manipulate stock prices by depicting false corporate announcements. Such financial fraud can destabilize markets and entities.[23]

[21] Manik Tindwani, "The rising menace of Deepfakes: Legal implications in India," retrieved from <*https://lawfoyer.in/deepfakes-legal-implications-in-india/*> visited on 16.12. 2023 at 5:40 pm.
[22] *Ibid*.
[23] Manik Tindwani, "The rising menace of Deepfakes: Legal implications in India," retrieved from <*https://lawfoyer.in/deepfakes-legal-implications-in-india/*> visited on 16.12. 2023 at 5:40 pm.

e. Phishing- Cybercriminals can use deepfakes to impersonate trusted individuals, such as company executives or family members, in video calls to deceive people into revealing sensitive information or transferring money.[24]

f. Blackmail- Criminals may use deepfake videos to create fake compromising content and then extort money from victims by threatening to release the fabricated material.

g. Identity Theft- Deepfakes can be used to impersonate someone for fraudulent activities or to gain unauthorized access to systems, as facial recognition systems can be deceived.[25]

RECENT INSTANCES OF DEEPFAKE

AI generated images and deep fake videos are an increasing threat to public discourse. There are many incidents that took place in India involving Deepfakes which left everyone shocked. In 2018, Journalist Rana Ayyub was victimized by a Deepfake porn plot. Her face was morphed into a pornographic video after she supported victim of Kathua gang rape. The mental agony such an incident can cause is beyond imagination.

Back in 2020, in the first-ever use of AI-generated deepfakes in political campaigns, a series of videos of Bharatiya Janata Party (BJP) leader Manoj Tiwari were circulated on multiple WhatsApp groups. The videos showed Tiwari hurling allegations against his political opponent Arvind Kejriwal in English and Haryanvi, before the Delhi elections. In a similar incident, a doctored video of Madhya Pradesh Congress chief Kamal Nath recently went viral, creating confusion over the future of the State government's Laadli Behna Scheme.[26]

Recently a video that purported to show Delhi Chief Minister Arvind Kejriwal intoxicated and slurring surfaced. A Pornhub user profile called black and white panda posted videos of

[24] Mijanul Kabir, "Cybercrimes on deepfake videos & the Indian Law," retrieved from <*https://mijanulkabir.com/cyber-crimes-on-deepfake-videos-the-indian-law/*> visited on 18. 12. 2023 at 4:06 pm

[25] *Ibid.*

[26] Aaratrika Bhaumik, "Regulating deepfakes and generative AI in India- Explained," retrieved from <*https://www-thehindu-com.cdn.ampproject.org/v/s/www.thehindu.com/news/national/regulating-deepfakes-generati ve-ai-in-india-explained/article67591640.ece/amp/?amp_gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#amp_tf=From%20%251%24s&aoh=17167242373546&referrer=https%3A%2F%2Fwww.google.com&amps hare=https%*3A%2F%2Fwww.thehindu.com%2Fnews%2Fnational%2Fregulating-deepfakes-generative-ai-in-india- explained%2Farticle67591640.ece> visited on 26.5.2024 at 5:27 pm.

Bollywood actresses. The videos come with a Deepfake disclaimer, but are hugely disturbing considering the non-consensual nature of them.

Deepfake videos of Rashmika Mandana, Katrina Kaif and Kajol have caused unrest around the world and they had to clarify that it was indeed a fake video. This technique can be seriously detrimental. A viral video featuring actress Rashmika Mandanna circulated widely on social media in November last year. In response, the actress promptly took to her social media platforms to express her distress.

Actress Priyanka Chopra was spotted endorsing a brand and disclosing her annual income in another misleading video. Unlike some other actors, Priyanka's face remains unaltered in controversial videos. However, the audio of her voice and lines from the original video have been substituted with a fake brand advertisement.

Similarly, actor Alia Bhatt was featured in a deceptive deepfake video later confirmed to be false. The viral footage showed Bhatt's face digitally placed onto another woman, depicted sitting on a bed.

Actor and dancer Nora Fatehi has fallen prey to the latest wave of deepfake videos. Taking to her Instagram story, Nora revealed that the technical apparel and athletic shoes website 'Lulumelon' had employed a deepfake video of her to promote the brand. [27]

The recent emergence of a Deepfake video featuring the Prime Minister of India (Shri Narendra Modi) participating in the rhythmic joy of Garba serves as a stark reminder of the expanding web of deception spun by advanced artificial intelligence. This incident, however, is not just a momentary spectacle but a chilling indicator of the broader, more insidious issue that this technology portends.

Earlier in December 2023, Ratan Tata, ex-chairman of the Tata Group, exposed a deepfake video on Instagram where he appears to give investment advice. The video, shared by user Sona

[27] Sangeeta Ojha, "From Ratan Tata, Sachin Tendulkar to Madusudan Kela: 9 well-known personalities who were victims of deepfake videos," retrieved from *<https://www-livemint-com.cdn.ampproject.org/v/s/www.livemint.com/news/india/from-ratan-tata-sachin-tendulkar- to-madusudan-kela-9-well-known-personalities-who-were-victims-of-deepfake-videos/amp-11710307982420.html?a mp_gsa=1&amp_ js v=a9&usqp=mq331AQIUAKwASCAAgM%3D>* visited on 26.05. 2024 at 5:50 pm.

Agarwal, falsely depicted Tata offering investment guidance, along with a caption suggesting users could amplify their investments 'risk-free'.[28]

In January 2024, renowned cricketer Sachin Tendulkar took to the social media platform X (formerly Twitter) to reveal that a deepfake video promoting a mobile application with his likeness is circulating on social media. He expressed his dismay at the widespread misuse of technology.

DEEPFAKE AND IDENTITY THEFT

In today's digital era, the emergence of Deepfake technology has revolutionized various aspects of media and communication. However, its implications extend far beyond entertainment, delving into the realm of identity theft. Deepfake, a technique that uses artificial intelligence to create realistic fake videos or images, poses a significant threat to individuals' identities and privacy.

Identity theft, traditionally characterized by the unauthorized use of someone's personal information for fraudulent purposes, has evolved with technological advancements. Deepfake amplifies the sophistication of identity theft by enabling the manipulation of audiovisual content to fabricate convincing impersonations of individuals. Through Deepfake, malicious actors can fabricate videos or images depicting someone engaging in activities they never did or uttering words they never said, thus tarnishing their reputation or perpetrating fraud in their name.

One of the most alarming aspects of Deepfake as a form of identity theft is its potential to deceive even the most discerning individuals. With advancements in AI algorithms, Deepfake technology can seamlessly replicate facial expressions, voice inflections, and mannerisms, making it increasingly challenging to distinguish between genuine and fabricated content. Consequently, unsuspecting individuals may fall victim to false accusations, defamation, or financial scams orchestrated using Deepfake-generated materials.[29]

Moreover, the proliferation of Deepfake content across social media platforms exacerbates the spread of misinformation and undermines trust in digital media. Fake videos or images created

[28] *Ibid.*
[29] Mika Westerlund, *op.cit*. 42.

through Deepfake can go viral within minutes, causing irreparable damage to an individual's reputation or credibility. As a result, victims of Deepfake identity theft may endure emotional distress, social ostracization, and professional setbacks, as their digital likeness is manipulated and exploited for malicious purposes.

Furthermore, the widespread availability of Deepfake tools and tutorials amplifies the accessibility of identity theft techniques to a broader spectrum of individuals, including o and amateur hackers. The democratization of Deepfake technology empowers malicious actors to perpetrate sophisticated identity theft schemes with relative ease, further exacerbating the prevalence and severity of digital impersonation incidents. To combat the escalating threat of Deepfake-enabled identity theft, concerted efforts from various stakeholders are imperative. Additionally, specific legislation dealing with the issue and public awareness is the need of the hour. Education initiatives focusing on media literacy and digital hygiene can equip individuals with the knowledge and skills needed to discern authentic content from Deepfake manipulations, thereby mitigating the risk of falling victim to identity theft.[30]

It is often seen that the main defence used against the fake content is that an individual on one hand has the freedom of speech and expression granted under Article 19 of the Constitution of India. The thing that is to be considered is that our freedom of expression ends where one's right to privacy begins. Our duty here is to understand that our actions and freedom does not tend to hamper any other individual's enjoyment of rights. The right to withholding an assent is a right guaranteed under Article 19 of Indian Constitution to every individual but the same can't be used to justify the creation and dissemination of fabricated or altered videographic content/still image that has the capability to manipulate people's thought process regarding the subject of the content. Hence, to combat this, the regulators and citizens should do their duty towards the welfare of the society.[31]

Thus, addressing the complex interplay between Deepfake and identity theft requires collaborative efforts from technology companies, policymakers, and the public to develop comprehensive strategies for detecting, preventing, and mitigating the impact of

[30] *Id*. at 47.
[31] Srishti Dey, *loc.cit.*

Deepfake-enabled impersonation incidents. Only through concerted action can we safeguard the integrity of our digital identities in an era defined by technological innovation and digital deception.

CONCLUSION

There is an old saying - "*Seeing is believing*". However, in the wake of the advancing deepfake technology, it could be dangerous for individuals as well as society to believe in what they view. Considering the fact that detection and regulatory measures concerning deepfakes are still in their nascent stage throughout the world, it is pertinent to be well aware of our technological and legal capabilities in the fight against this hazard.[32]

This new AI technique may have better prospects, however, we cannot ignore that there are more misgivings than credence to the use of deepfakes. The viable solution to this cyber threat is combination of technology and legislation.[33] The problem of DeepFake is developing more rapidly than even thought. Soon, it's going to get to the point where there is no way that we can actually detect Deepfakes anymore, so there is a need to look at other types of solutions.[34]

IJERTAs de Ruiter states that- "Deepfake technology and Deepfakes are morally suspect, but not inherently morally wrong". In her opinion, three factors condition the immoral use of Deepfakes- representation of persons to which they would not consent, deliberate deception of viewers, and harmful intention. Considering these specific factors, morally acceptable use of deepfakes is not entirely out of the question.[35]

[32] Nisha Dhanraj Dewani, Zubair Ahmed Khan. *(eds.), etal*., *Handbook of Research on Cyber Law, Data Protection, and Privacy* (USA: IGI Global, 2022) 37.
[33] Purvi Nema, "Are Indian Laws Equipped To Deal With Deepfakes?," retrieved from <*https://jils.blog/2020/07/19/are-indian-laws-equipped-to-deal-with-deepfakes*/> visited on 10.5.2024 at 10:30 pm.
[34] Hao Li, Deepfake Pioneer & Associate Professor.
[35] Andreas Eberl, Juliane Kuhn. *etal.*, "Using deepfakes for experiments in the social sciences - A pilot study,"
Frontiers in Sociology, Vol.7 (November 2022).