Page 1324- 1336 **DOI:** *https://doij.org/10.10000/IJLSI.112058*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 3

2024

© 2024 *International Journal of Legal Science and Innovation*

Follow this and additional works at: https://www.ijlsi.com/

Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com)

This Article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact **Gyan@vidhiaagaz.com.**

To submit your Manuscript for Publication at **International Journal of Legal Science and Innovation**, kindly email your Manuscript at **editor.ijlsi@gmail.com.**

The East & West of Deepfakes: A Comparative Study of Laws in India & UK

SHRADDHA PANDIT[1] AND JIA SINGH[2]

ABSTRACT

Deepfakes are a form of synthetic media that utilize deep learning and artificial intelligence techniques to create or modify content, such as audio, video, or images, in order to appear genuine and authentic. The term "deepfake" is derived from the combination of "deep learning" and "fake." The technology behind deepfakes relies on neural networks, specifically generative adversarial networks (GANs) or autoencoders, to analyze and replicate patterns from existing data, such as movies or photographs of a specific individual. This enables deepfakes to manipulate speech or facial expressions, replace faces in videos, and generate content that is difficult to distinguish from real and unaltered media. While deepfake technology has potential applications in industries like entertainment and visual effects, it has also raised concerns due to its potential for misuse. Deepfakes can be used to create convincingly fake videos with malicious intent, such as spreading false information, fabricating news, or producing explicit material involving unsuspecting individuals. In India and the UK, the growing use of deepfake technology has highlighted the need for stronger legal frameworks to address issues related to privacy, data protection, and cybercrime. While existing laws can be utilized to combat deepfakes, specialized legislation specifically targeting the challenges posed by deepfakes is necessary in the current landscape. Deepfakes have emerged as a significant cyber threat in India, particularly targeting popular figures such as actors, celebrities, and sports personalities. This threat affects individuals across various demographics, regardless of age, gender, religion, class, or social status. It is time that countries join hands across borders to lessen the negative impact of and eventually eliminate cyber-crime and deepfake technology.

Keywords: *Deepfake, cyber-crime, CEDAW, UN SDGs, ICT*

I. MEANING & INTRODUCTION

Deepfakes are a subset of synthetic media in which content usually audio, video, or image is created or altered using deep learning and artificial intelligence (AI) techniques to look real and authentic. "Deep learning" and "fake" are the sources of the word "deepfake."

[1] Author is an Assistant Professor of Law & Ph.D. Candidate at SVKM's KMPSOL, NMIMS Deemed to be University, Mumbai campus, India.
[2] Author is a student at Guru Gobind Singh Indraprastha University, Delhi, India.

© 2024. International Journal of Legal Science and Innovation [ISSN 2581-9453]

Deepfake technology makes use of neural networks, namely generative adversarial networks (GANs) or autoencoders, to identify and replicate patterns from pre-existing data, including movies or photos of a certain individual. Deepfakes can be used to alter speech or facial expressions, substitute faces in videos, and produce information that might be hard to tell apart from authentic, untouched media. Deepfake technology has generated worries because of its possible misuse, even if it has potential uses in a variety of industries, including entertainment and visual effects. Deepfakes can be used to produce convincingly fake videos for nefarious ends, such as disseminating false information, fabricating news, or even producing explicit material with gullible people.

Experts state that there are several advantages of deepfake technology such as:

Entertainment, Creative Expression and Animation:

Deepfakes have paved the way for highly advanced applications in various fields like advertising, creative arts, and film productions[3]. They allow filmmakers, artists, and content creators to manipulate and transform existing footage, creating new and imaginative content. Actors can be digitally rejuvenated or de-aged, enabling them to play roles across different time periods. They help to enhance visual effects in movies, TV shows, and video games, thus improving the overall viewing experience.

Training and Simulation:

Deepfakes can be used for training simulations in various fields, such as medicine, aviation, and military. Medical students can practice surgeries on simulated patients, and pilots can train in realistic flight scenarios.

Historical, Preservation, Education and Accessibility:

Deepfakes can bring historical figures to life by animating old photographs or paintings. Educational institutions can use them to create engaging and interactive lessons. Deepfakes can help people with disabilities by providing sign language interpretation or lip-syncing for speech-impaired individuals.

However, the increased use of deep fakes is equally intimidating and raises ethical and security concerns. The swift progress of deepfake technology has prompted heightened endeavors to create instruments for identifying and alleviating the effects of deepfakes, along with ethical deliberations over its application and possible ramifications.

[3] Deepak Dagar & Dinesh Kumar Vishwakarma, 'A literature review and perspectives in deepfakes: generation, detection, and applications' 2022 Int J Multimed Info Retr **11**, 219–289 https://doi.org/10.1007/s13735-022-00241-w accessed 12 April 2024

II. DEEPFAKE MENACE IN INDIA & APPLICABLE LAWS

Coming to India, concerns regarding the need for more robust legal frameworks to address issues like privacy, data protection, and cybercrime have been highlighted by the growing usage of deepfake technology. Although India has laws that can be used to counteract deepfake technology, additional specialized legislation is required to address the particular issues that deepfakes pose in the current times. Deepfakes are an emergent cyber threat in India, where largely popular faces, actors, celebrities and sports persons are the soft targets of the said technology. The threat of deepfake has spared none, irrespective of age, gender, religion, class or social status.

Identity theft and virtual forgery

Using deepfakes for virtual forgeries and identity theft can be serious offences with substantial repercussions for both individuals and society at large. Deepfakes can damage a person's reputation and credibility and disseminate misleading information if they are used to steal someone's identity, inaccurately portray them, or sway public opinion.

In 2023 an elderly man, a septuagenarian from the Kerala state in India, fell victim to a video call made by using deepfake technology[4]. The scammer impersonated the victim's former colleague, whereby the voice and face of the former colleague was matched. Relying on the video, the victim made a transfer of money into an account in another Indian state. The authorities have been investigating the matter in depth. However, this case has been considered to be the first reported case of deep fake monetary scam in India.

In January 2024, a recent victim of the deepfake technology was the reputable and respectable Indian Cricketer, Sachin Tendulkar[5], who was seen promoting an online game with an example of his daughter, Sara Tendulkar earning Rs. 1.8 lakh per day by making predictions.

As per Indian law, the Section 66[6] , Section 66-C[7] and Section 66-D[8] of the Information Technology Act, 2000, all these cyber-crimes can be prosecuted. Similarly, the Sections 420[9],

[4] VISHNU VARMA, 'KERALA MAN LOSES ₹40K TO AI-ENABLED DEEP-FAKE FRAUD', THE HINDUSTAN TIMES (KOCHI, 18TH JULY 2023)
[5] Nikhila Henry, 'Sachin Tendulkar: Indian Cricket Legend Flags 'disturbing' deepfake video' BBC News (Delhi, 16th January 2024)
[6] Section 66 of IT Act, 2000, Computer related offences, India Code https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=76
[7] Section 66C of IT Act, 2000, Punishment for Identity Theft, India Code https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=79
[8] Section 66-D of IT Act, 2000, Punishment for cheating by personation by using computer resource https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=80.
[9]Section 420 of IPC, 1860, Criminal Offence of Cheating and dishonestly inducing delivery of property, India Code https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00037_186045_1523266765688&sectionId=46203&sectionno=420&orderno=477

Section 468[10] and Section 469[11] of the Indian Penal Code, 1860 could also be invoked in this regard.

Invasion of privacy, rise of sexual offences and defamation

In India, the Right to Privacy of an individual is included in Article 21, i.e. Right to Life and Personal Liberty. However, deepfakes make the fundamental right to privacy completely groundless. The major obstacle is likely to arise in the pursuit of justice by a victim while claiming his or her fundamental right to privacy, whereby his or her privacy is invaded due to unlawful use of personal images and data. The major hindrance in achieving justice is the difficulty in distinguishing between real and deepfake images and videos. Section 66-E[12] of the Information and Technology Act, 2000 can be applied in this regard.

Another major issue in current times is 'Revenge Porn'. This term 'revenge porn' refers to the distribution of sexually explicit images or videos of individuals without their consent. There has been a significant increase in dissemination of revenge porn non-consensual content of a person by a former spouse or partner of that person, in order to cause mental trauma, defamation, social embarrassment, distress and loss of reputation. This is done with the help of advanced deep fake, artificial intelligence and cyber technology. Such illegal activities and cyber crimes are not only violate women's right to privacy but also lead to a rise in crimes against minor children, which are quite alarming and pose a danger to the entire human society at large.

Section 67-B[13] of the Information Technology Act, 2000 can be invoked for curbing deepfakes contributing to sexual offences against children. To defend the rights of women and children, it is also possible to refer to Sections 292[14] and 294[15] of the Indian Penal Code, 1860, which

[10] Section 468 of IPC, 1860, Criminal Offence of Forgery for purpose of Cheating, India Code https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00037_186045_1523266765688&sectionId=46251&sectionno=468&orderno=525#:~:text=Whoever%20commits%20forgery%2C%20intending%20that,also%20be%20liable%20to%20fine.

[11] Section 469 of IPC, 1860, Forgery for purpose of harming reputation, India Code https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00037_186045_1523266765688&orderno=526#:~:text=Whoever%20commits%20forgery%2C%201%20%5Bintending,also%20be%20liable%20to%20fine.

[12] Section 66-E of IT Act, 2000, Punishment for violation of privacy, India Code https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=81#:~:text=Whoever%2C%20intentionally%20or%20knowingly%20captures,two%20lakh%20rupees%2C%20or%20with

[13] Section 67-B of IT Act, 2000, Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form, India Code https://www.indiacode.nic.in/show-data?abv=CEN&statehandle=123456789/1362&actid=AC_CEN_45_76_00001_200021_1517807324077&sectionId=13094&sectionno=67B&orderno=85&orgactid=AC_CEN_45_76_00001_200021_1517807324077

[14] Section 292 of IPC, 1860, Sale, etc., of obscene books, etc., India Code India Code: Section Details

[15] Section 294 of IPC, 1860, Obscene acts and songs., India Code India Code: Section Details

deal with punishment for the sale of pornographic material) as well as Sections 13, 14, and 15 of the Protection of Children from Sexual Offences Act, 2012 (POCSO) which provides for stringent punishment procedures for child pornography.

Online defamation and hate speech using deepfake technology may create serious issues that harm individuals as well as raise public concern. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 made under the Information Technology Act, 2000 stipulate the legal penalties for these offences. In addition, Sections 153-A and 153-B (Speech damaging public tranquillity) and Section 499 (defamation) of the Indian Penal Code, 1860, may be invoked in such legal scenarios.

The Ministry of Electronics and Information Technology has issued in its latest Advisory dated November 07, 2023, directing the significant social media the following[16]:

- "Ensure that due diligence is exercised and reasonable efforts are made to identify misinformation and deepfakes, and in particular, information that violates the provisions of rules and regulations and/or user agreements and
- Such cases are expeditiously actioned against, well within the timeframes stipulated under the IT Rules 2021, and
- Users are caused not to host such information/content/Deep Fakes and
- Remove any such content when reported within 36 hours of such reporting and
- Ensure expeditious action, well within the timeframes stipulated under the IT Rules 2021, and disable access to the content/information."

The intermediaries were warned that any act in contravention of the concerned provisions of the Information Technology Act, 2000 and Rules would attract Rule 7 of the Information Technology Rules, 2021 and could render the organization liable to losing the protection available under Section 79(1) of the Information Technology Act, 2000. In addition, under Rule 3(2)(b) of the Information Technology Rules, 2021, deepfake has been classified as impersonation and misinformation and therefore has detailed provisions on the actions to be taken for the violators.

Misinformation against Governments

It is a severe problem that can have far-reaching effects on society when deepfakes are used to propagate false information, undermine the government, or foster animosity and

[16]Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes, Ministry of Electronics and IT pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445

disenchantment with the government. The dissemination of incorrect or misleading information has the potential to sway public opinion, erode public confidence, and affect political outcomes. Cyberterrorism offences fall under the purview of Section 66-F of the Information Technology Act of 2000, as well as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2021[17]. Also, Section 121 (waging war against the Government of India) and Section 124-A of the Indian Penal Code, 1860 could be cited.

The deployment of deepfakes has the potential to seriously impact outcomes and jeopardize the integrity of the democratic process. Deepfakes have the potential to sway public opinion, impact election results, and disseminate inaccurate or misleading information about political candidates. A lot of governments and organizations are acting to address the growing worry over the influence of deepfakes on elections. Section 66-D of the Information Technology Act of 2000, which deals with the punishment for cheating by personation utilizing computer resources, and Section 66-F, which deals with cyber terrorism, allow for the prosecution of these crimes.

III. DEEPFAKE MENACE IN THE UK & APPLICABLE LAWS

Coming to the West, UK is channelising towards a safer path since the Online Safety Act, 2023 has received the Royal Assent and is at present in effect as of October 26, 2023[18]. This legislation aims to address various online harms and threats to the users, including deepfake porn. In the words of the Technology Minister, Michelle Donelan, "It will make the UK the safest place to go online."

Since the year 2024 is billed as a huge year for democracy, the Members of Parliament across Westminster show a deep concern about deepfakes as a means to undermine the integrity of the democratic elections. A survey of Members of Parliament reveals that 70% of them fear the spread of misinformation and disinformation as a consequence of artificial intelligence as in recent months, London Mayor, Sadiq Khan and Labour Party Leader, Keir Starmer have been the targets of deepfakes[19].

The key points regarding deepfakes under the Online Safety Act, 2003 include:

[17] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics and IT, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated 06.04.2023)-.pdf (meity.gov.in)
[18] ONLINE SAFETY ACT 2023, LEGISLATION.GOV.UK ONLINE SAFETY ACT 2023 (LEGISLATION.GOV.UK)
[19] CALL FOR ACTION ON DEEPFAKES AS FEARS GROW AMONG MPS OVER ELECTION THREAT, THE GUARDIAN (UK, 21ST JANUARY 2024)

1. **Recognition of Harm**: The Act designates deepfake porn as a type of digital sexual assault and recognizes it as legally offensive and hurtful.

2. **Criminalization**: Sending or disseminating deepfake pornography is prohibited by the Act. This implies that those who partake in such actions may be subject to legal repercussions, including possible incarceration.

3. **Social Media Platform Responsibilities**: There are now strict obligations on social media platforms regarding unlawful information. They must take proactive measures to combat crimes such as harassment, controlling or coercive behavior, and revenge pornography. The platforms risk incurring hefty fines if they don't comply.

4. **New Offences**: The Online Safety Act establishes four new offences, one of which is the prohibition of the unconsented sharing of intimate photos, which also includes deepfakes.

5. **Closing a Loophole:** The Act acknowledges a previous legal loophole by permitting prosecution without requiring proof of intent to cause embarrassment or distress. Regardless of the motivation, the conduct itself shall have legal repercussions.

6. **Maximum Sentence**: The spreading of deepfake pornography is an offence punishable with imprisonment for a maximum term of two years.

7. **Combatting Sexual Abuse**- The Act has tightened the law concerning sexual abuse. Whether the images are real or fake, the Act simplifies punishing someone for sharing private photos without permission. Additionally, the non-consensual dissemination of pornographic deepfakes is prohibited by the new law. If proven guilty of disseminating these pictures, the maximum sentence for jail time is six months. This is a landmark breakthrough in which the victim does not need to provide proof that the offender intent to cause them discomfort.

The communications regulator Ofcom oversees the new Act. Ofcom has the authority to fine social media companies up to £18 million, or 10% of their global yearly turnover if they do not sufficiently follow the rules outlined in the Online Safety Act.

Former Justice Secretary Sir Robert Buckland urged the government to take efforts to tackle what he sees as a "clear and present danger" to the UK[20]. The National Cyber Security Centre (NCSC) warns in its report the following, "Large language models will almost certainly be used to generate fabricated content, AI-created hyper-realistic bots will make the spread of disinformation easier and the manipulation of media for use in deepfake campaigns will likely

[20] BRIAN WHEELER & GORDON CORERA, FEARS UK NOT READY FOR DEEPFAKE GENERAL ELECTION, BBC NEWS, (UK, 21st December 2023)

become more advanced."

IV. APPLICATION OF CEDAW & UN SDGS

Understanding the importance and need of an international law in relation to wipe out all sorts of crime, violence and differentiation against women, the United Nations General Assembly adopted the "Convention on the Elimination of All Forms of Discrimination against Women" (CEDAW) on 18th December 1979[21]. It is often referred to as the most important document for securing women's rights, gender equality and the "International Bill of Rights for Women". It targets cultural and traditional norms as influential forces shaping gender roles and family relations. CEDAW has provided the firm foundation for judicial decisions, legal and policy frameworks at the country level.

Use of deep fake against women is a kind of 'cyber violence' against women. The Fourth United Nations World Conference on Women held in Beijing in 1995 stated that violence against women (VAW) is a manifestation of the historically unequal power relations between men and women. Therefore, despite most countries of the world having their own national laws and the existence of UDHR and CEDAW and having several debates and discourses on the topic, time and again the newspapers do get plagued with news pieces about how women's right to privacy gets violated due to deep fake and revenge porn.

This points out to the fact that societal attitudes and stereotypes against women have not changed much even in the current times, when the global discourse on gender justice is in vogue. The evil of cybercrime, deep fake and revenge porn not only hampers women's rights but also impedes the healthy and balanced development of any society and nation. A paradigm shift in attitudes is required to take the Indian society, economy and family from rigid patriarchy towards a balanced gender equitable society. Urgent gender-sensitization is required. If technology, sociology and law-making are utilised in a symbiotic way, they will also ultimately contribute to achieving "GOAL 5: Gender Equality", which is one of the United Nations Sustainable Development Goals. This goal aims to achieve an end to all types of discrimination against women and girls and is to be globally achieved by 2030.

[21]Dubravka Šimonović, Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) for Youth, UN WOMEN, United Nations Audiovisual Library of International Law Introductory Note - Dubravka Šimonović, Chairperson of the Committee on the Elimination of Discrimination against Women (2007-2008) - English (un.org)

V. CONCLUSION & RECOMMENDATIONS

In India:

Laws need to live up to the ever evolving and fast-moving technology, which is not only intimidating and challenging but also an extensive process. Making changes in existing laws by amendments requires a lot of time and precision. However, deep fake technology just updates itself at a very great speed without losing any time.

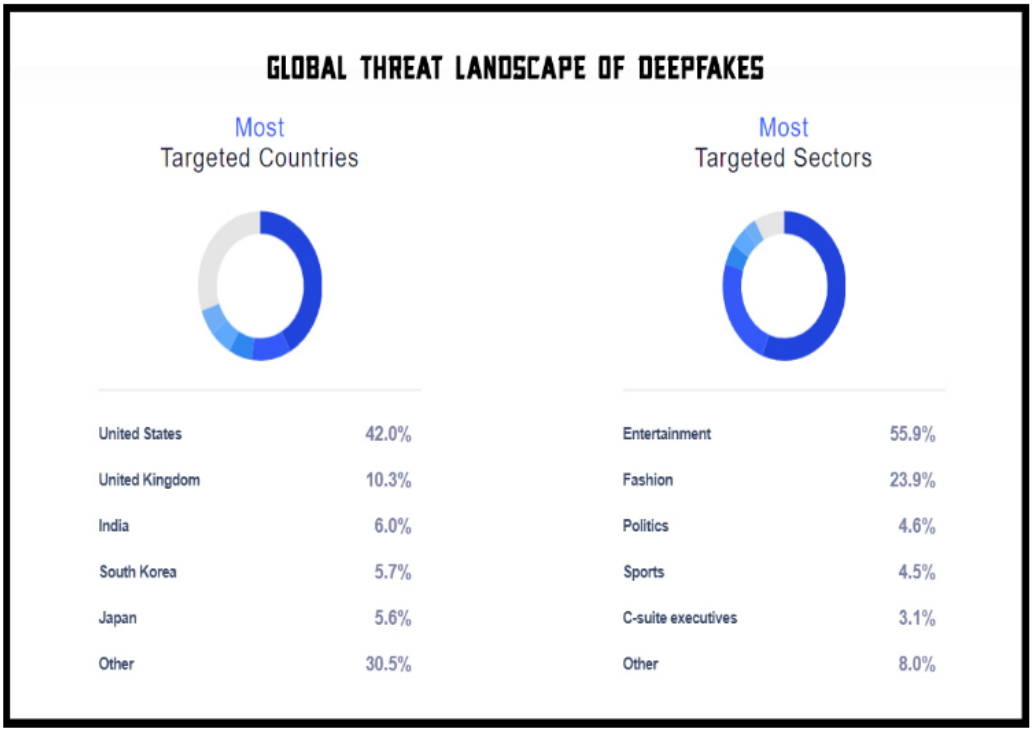
Although there are several laws in India, the implementation of these laws needs improvement. The Information and Technology Act, 2000 does not explicitly provide the penalty of making and sharing deepfakes. At present, the offence of deepfake can be arisen in corroboration with existing provisions of the different laws. The foremost lacuna arises due to the absence or lack of statutorily acknowledgement of the word “deepfake” and the acts that comes within the purview of deepfake. This creates an impediment to prosecute the perpetrators.

Also in recent times, the social media and internet intermediaries has proposed before the government to only remove content which was released with “criminal or ill intent”. These intermediaries have argued that if all the deepfake content is removed, it could likely mean an end of life for innovation or generation of new kinds of content in advertising and marketing. Consequently, the government intends that only if the content is ‘misleading’ it should be barred. This connotes that if the content has only an entertainment value, it is harmless, and need not be removed, which again creates a grey area and raises several ethical questions such as what amounts entertainment in current times and what amounts to digital privacy? The jurisprudence of deep fake and revenge porn is not developed completely yet, but this area of research and legal study needs to be dealt with in a socio-legal perspective and not just in a techno-legal one.

It is pertinent to quote the words of India Future Foundation founder and CEO Kanishk Gaur, he said, “Legislation must evolve to criminalise the malicious crafting and distribution of deep fakes, deterring would-be offenders. Moreover, public awareness campaigns and the advancement of detection technologies are critical in building a resilient digital defence. And given the borderless nature of the internet, international cooperation is paramount in this endeavour.”

In fact, it is not that there is an increase in deep fake and revenge porn cases only in Asia or India. There have been several of USA’s Hollywood's leading actresses being "Deepfaked”, so

that subscribers of porn sites could swell to 80,000 in only in a matter of few months[22]. These deep fake videos are marketed as "hacked" or "stolen" which is an effective excuse to escape liability. Such cyberspace activities leave deep scars on the victims' psyche, at times beyond compensation and repair. Thus, the Psychological Impact Assessment is required of victims of cybercrimes, deep fake and revenge porn. At the same time, the perpetrators should not only be caught and punished but also made to pay compensation or damages to their victims.



(Image credit: sensity.ai)

In the UK & its Island territory, St. Helena:

Section 170 of the Online Safety Act proposes a new section 66A in the Sexual Offences Act, of 2003:

"66A Sending etc photograph or film of genitals

(1) A person (A) who intentionally sends or gives a photograph or film of any person's genitals to another person (B) commits an offence if—

(a) A intends that B will see the genitals and be caused alarm, distress or humiliation, or

(b) A sends or gives such a photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether B will be caused alarm, distress or humiliation

[22] Alec Banks, 'Op-Ed Deepfakes & Why The Future Of Porn Is Terrifying' Highsnobiety.com What Are Deepfakes & Why the Future of Porn is Terrifying (highsnobiety.com)

(5) References to a photograph or film also include—

(a) an image, whether made by computer graphics or in any other way, which appears to be a photograph or film"

Thus, the Act does not define or prohibit the making and sharing of "deepfakes". It is the "mens rea" (criminal intention) of the sharer and the potential "alarm, distress, or humiliation" caused to the victim that makes it illegal. The law only criminalizes deepfake concerning pornography, and not otherwise. Anyone who has had their intimate content shared online without consent is not protected to have that content removed from the internet, even if the perpetrator has been brought to justice. This is because of the reason that the content is not classified as "illegal per se".

It is to the disappointment that despite the affirmative steps forward, the victim is not completely shielded by the law, and has to endure the aftermath of the offence by the perpetrator. While it is illegal to share sexual deepfakes in the absence of consent, there is still no law that prevents such material from being created in the first place. Several new offences are also included in the Act which tackle image-based sexual abuse, in the forms of cyberslacking and the sharing of deepfake pornography, however, the major lacuna is that the creation of deepfake porn is not yet completely outlawed.

The examination of deepfake laws in India and the UK highlights both commonalities and distinctions in their strategies for tackling the problems caused by the manipulation of synthetic media. Several significant conclusions from this study are acknowledged, including the way legislation is responding to the changing landscape of technology.

1. **Specific Legislative Framework:** Legal action against deepfakes is recognised as necessary in both India and the UK. A separate legislation on penalising deepfakes becomes necessary to effectively deal and deter the menace of deepfake. With a separate legislation, legal safeguards for victims of deepfakes can be enhances and a robust mechanism for the prosecution of the perpetrator can be developed. The unique legal traditions and cultural values of each nation, however, are reflected in the differences in the particular legislative frameworks.

2. **Penalties and Criminalization:** The research shows disparities in the laws that prohibit the production, dissemination, and intentional harm of deepfakes. It seems that the UK has a more thorough legal system with distinct punishments for various deepfake-related offences.

3. **Privacy and Consent:** Both nations stress the value of consent and privacy, but to different degrees the current legal frameworks sufficiently address these issues. The United Kingdom may offer more comprehensive protections for individuals due to its strict data protection

© 2024. International Journal of Legal Science and Innovation [ISSN 2581-9453]

regulations.

4. **Enforcement Mechanisms:** Deepfake rules must be effectively enforced in order to be put into practice. According to the report, the UK might have more well-established enforcement mechanisms, such as specialised authorities and well-defined protocols.

5. **Technology-Related Issues**: The swift advancement of deepfake technology demands a proactive legal strategy. To stay up with evolving challenges and technological improvements, both India and the UK must update their legal systems regularly.

6. **International Collaboration**: International cooperation is crucial given the worldwide reach of digital information and the internet. Both nations ought to look for ways to work together to solve the cross-border issues brought on by deepfakes.

7. **Public Awareness and Education**: An effective plan to counter deepfakes must include both public awareness and education. People believe in deepfake videos or pictures due to the lack of education in distinguishing between real and fake. There is still a larger segment of the population who are not aware of the emergence of a new cyber threat named deepfakes and the aftermath of the threat. Thus, India and the UK ought to make significant investments in educational programs to empower individuals to recognize and effectively respond to synthetic media.

With the growing usage of internet, national boundaries are vanishing. The result is that cyber-crime is becoming a part of everyday life. It is also very difficult to locate and catch hold of the cyber criminals and creators of deep fake and revenge porn. There is a possibility that the perpetrator may not be a single individual but an organised crime syndicate. When it is done by group of offenders operating from remote locations, it thwarts attempts by countries to prosecute cyber-crimes committed against victims within their national boundaries. When prosecution does occur, it is typically only because of creativity on the part of prosecutors[23].

It is also possible that the reduction of trust in news on social media resulting from the uncertainty induced by deceptive deepfakes may not generate cynicism and alienation, but scepticism amongst the public[24]. If people rely on unregulated deep fake videos on social media, they might not believe in the news they see and might even question governmental policies and schemes, thus leading utter confusion and chaos.

[23] Raymond R. Panko, 'Corporate Computer and Network Security', Pearson India, 2009. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/mpstme/detail.action?docID=5126793.
[24] J. N. Cappella & K. H Jamieson, 'News frames, political cynicism, and media cynicism'. *The Annals of the American Academy of Political and Social Science,* 546(1), 71–84. (1996).

Coming to the small island territory of UK, St. Helena in southern Altantic ocean, there is some good news as the Government of St. Helena has taken cyber security issues and cybercrime very seriously. The Government there ensures staff training and awareness of cyber security which plays a significant role in securing the ICT systems and data[25]. This also helps to shield against cyber-attacks. Therefore, all the staff undergo mandatory cyber security training and are periodically reminded of good cyber hygiene practices through cyber security awareness campaigns, including distribution of educational posters, weekly cyber security tips sent via email, as well as short online training modules, which serve as refreshers to the initial training they receive. These campaigns usually utilise popular social media channels and platforms, local newspapers and radio stations in order to raise awareness amongst the general public of St Helena. As the way forward, the Government also plans to develop these public campaigns further by providing updates on the SURE Promotional Channel as well as hopes to conduct periodic public cyber security training workshops. As they believe in "Prevention is better than cure". Most countries of the world can learn from the Government of St. Helena.

The most recent announcement made by the UK Government on 16th April 2024 has brought some relief for women, that is a new offence, which will be introduced through an amendment to the Criminal Justice Bill, will mean anyone who makes sexually explicit deepfake images of adults maliciously and without consent will face the consequences of their actions. The government has also re-classified violence against women and girls as a 'national threat', meaning the police must prioritise their response to it, just as they do with threats like terrorism - as well as ongoing work to tackle image-based abuse[26].

To conclude, whether it be the East or the West, in order to effectively handle the various issues offered by deepfakes, the comparative analysis at hand highlights the necessity of continued efforts in legislative refinement, technological adaptation, and international cooperation. There must be setting up of a global police for preventing deepfakes and reducing cybercrimes (like a specialised cyber wing of the INTERPOL), thereby overcoming linguistic, geographical, cultural and jurisdictional barriers and delivering justice. Law and policy makers need to be alert in adjusting their strategies to safeguard people and society from the possible risks connected with manipulating synthetic media as the legal environment changes.

[25] SHG Cyber Security, ST. Helena Government SHG Cyber Security | St Helena Government (sainthelena.gov.sh)

[26] LAURA FARRIS MP & MINISTRY OF JUSTICE, GOVERNMENT CRACKS DOWN ON 'DEEPFAKES' CREATION, GOV.UK (UK, 16TH APRIL 2024) GOVERNMENT CRACKS DOWN ON 'DEEPFAKES' CREATION - GOV.UK (WWW.GOV.UK)