The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

# Ethical & Legal Implications of Deep Fake Technology: A Global Overview

*** Dr. Shashank Shekhar**
Assistant Professor (Law), Dr. Ram Manohar Lohiya National Law University, Lucknow,
E-mail: shashank1008@gmail.com
**Mr. Ashish Ransom**
Assistant Professor, Department of Law, Assam University, Silchar **-cum-** Research Scholar (Ph. D) at Dr. R. M. L. National Law University, Lucknow,
Email: ashish.ransom@gmail.com.

**Abstract**
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. Although political deep fakes are a new concern, pornographic deep fakes have been a problem for some time. These often purported to show a famous actress or model or any other woman, involved in a sex act but actually show the subject's face superimposed onto another woman's body who is actually involved in that act. This feature is called face-swapping and is known as the simplest method of creating a deep fake. There are numerous software applications that can be used for face-swapping, and the technology used is very advanced and is accessible. Deep fakes raise questions of personal reputation and control over one's image on the one hand and freedom of expression on the other. This will have a significant impact on user's privacy and security. Increasingly, governments around the world are reacting to these privacy evading applications for e.g., India banning TikTok and the USA investigating the privacy issues of TikTok and in the process of enacting laws to reduce the impact of deep fakes in the society. The study in this paper includes the ethical and legal implications surrounding the deep fake technology which also includes the study of several international legislations and analysing the position of India in tackling the crime of deepfake.
**Keywords:** Deepfake, artificial intelligence, data protection, privacy, ethical implications, legal implications, legislations, European Union, India,

## 1. Introduction

The world has seen ex President of America, Mr. Barack Obama calling Donald Trump names (badmouthing), one of the big tech player, another video where, Mr. Mark Zuckerberg declaring on having a "total control on billions of people's stolen data", and witnessing Jon Snow's moving apology for the unexpected and boring ending to Game of Thrones, all of these are products of deepfake. Deepfake uses a kind of artificial intelligence that is called deep learning to fabricate or alter images of fake evens, and hence the name as deepfake.

Synthetic media is a term where artificial intelligence algorithms are used for the modification, manipulation and artificial production of data by automated means. The deep fakes 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. These clips, which feature fabricated, altered and fake footage of people and things, are a growing concern in human society. Although political deep fakes are a new concern in the scene, pornographic deep fakes have been a serious concern recently.The act of digitally stitching one's face to another's body is called face-swapping and is known as the simplest method of creating a deep fake. There are many software applications and websites that provide a platform for face-swapping, and the technology used is very advanced and is accessible. Deep fakes raise questions of individual reputation and

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

control over one's privacy on the one hand and freedom of expression on the other. This will have a significant impact on user's privacy and security. European Union and several Governments around the world can be seen taking cognizance to analyse the harm it possesses and regulate the same.

## 2. Challenges Of Deepfakes

Deepfakes are a major threat to human society as a whole. Deepfakes are capable of contributing towards creating fake news to threaten national security by interfering in elections by disseminating fake propagandas on online platforms. The challenges that this technology possesses are really threatening.

Before categorising the challenges, first lets track down who produces deepfakes?[1] :

1) Deepfake hobbyists - Deepfake hobbyists communities 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 videoslike 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 one of the candidates prior to days before voting starts.[2] These hobbyists tend to see this kind of artificial intelligence generated videos as a new form of tech-art and use them to contribute towards online humor and look towards the development of such technology for solving out intellectual puzzles instead of using it to trick or threaten people. Whereas, some of them use it for their concrete personal benefits, such as for raising social awareness regarding the deepfake technology and the threats it possesses, whereas, they use it as art in order to get deepfake related work for several music videos, video games, advertisements or tv shows.

2) Political players - Political players, here 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 already have their hand in this threatening technology where artificial intelligence technology is used 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.

4)Entertainment Companies - Deepfake technologies are used by several game developers to give face to the game characters, followed by using this technology in several music videos and movie scenes. These are used with the sole purpose of encouraging and showcasing the art of movie making.

The deepfake technology is hereby backed by several challenges, which are further categorised in to - a) Ethical challenges b) legal challenges

### a) ETHICAL CHALLENGES

This technology gained popularity in the last few years, in December 2017, a social media user named as pseudonym 'deepfakes' showed the world how stitching faces digitally and using them maliciously is possible with the help of artificial intelligence techniques based on neural networks. Deepfakes then slowly gained popularity through funny and strange videos of famous showbiz celebrities and political figures on social media applications which were hard to believe to be unreal. Deepfakes have been recently receiving condemnation from around the globe for using of the technology for generating fake celebrity sex tapes, fake videos of politicians, financial frauds and revenge porn.

Some of the ethical challenges that this technology possesses can be categorised under Political challenges and Social challenges -

**Political Challenges** -

1) Political misinformation - World has witnessed several attempts of fake videos having a politician or public officer speaking his mind out and the video getting viral on social media platforms, with a malicious intent which had the capability to cause distress and spread fake information like fire in the land among the people. Fake political content created by using deepfake technology is a danger to society. Social media platforms like

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

Facebook have been in constant pressure to remove the deepfake content from its platform. For example, a fake video of Obama badmouthing Donald Trump in 2018.[3].

2) Deep Fake news - The journalism industry can be seen as a sufferer here due to its inability to saturate the fake and real content before broadcasting it to its viewers. The traditional fake news pose a lesser threat than the deepfakes do because they are harder to be detected and people believe what they see as real. The technology is capable of producing seemingly legitimate news videos that place the reputation of the news agency.
Nowadays, a race to be the first one to provide the news to its viewers and to access the video footage shot by a witness of an incident can provide a competitive advantage to a news media agency and hence, to be the top one in the race they often miss out to verify if the footage is real or fake.[4] Wrongly attributed video footages of protest videos, accident videos, fake protest speeches and etc with wrong caption to suggest it happened somewhere else and shall raise concern somewhere else. For example, Reuters in New Zealand during the Christchurch mass shooting came across a viral video on the internet that claimed to show the moment where the suspect was being encountered by concerned security officials. However it was further discovered that the footage was actually from the USA and the suspect of the Christchurch mass shooting was not yet killed.[5]
3) National Security - Times are gone when the wars were fought with weapons and soldiers were deployed on war zones, followed by destruction of life and property. In this era of evolving artificial intelligence, wars are being fought on cyber space and with technology. Foreign interference with the elections and using this technology to spread fake political propaganda and disrupting election campaigns simply by releasing videos that go viral, and are done merely by putting new words in mouth of someone who's in powerful public position with intent to cause riots, violence, unrest, doubt and distress among the voters is a powerful weapon in today's fake information war.

**Social Challenges** -

1) Non-consensual and revenge porn - The dark side of deepfakes, namely non-consensual and revenge porn, this technology enables the use of faces that are available online to be used in pornographic content without their consent. Here the famous celebrities are often the victims of non consensual porn that are created using the deepfake technology. Revenge porn using deepfake has the potential to violate victims' right to her own images and privacy, which is indeed a major concern.
2) Financial Fraud and Cybercrime: Here, the perpetrators often seemed to target CEOs using this deepfake technology, where it can make the victim say anything that he or she never said. Criminals could release a fabricated video that depicts a CEO falsely making comments that could affect the stock price of the company to fall while the perpetrators benefit from the short sales. This is a growing concern in financial fraud and white collar cybercrime in near future.[6]
3) Human sounding synthetic voice - Reports suggest that Google's is up with its efforts to develop voice assistant features that would be capable of mimicking human voice and with its addition to make and receive calls. Although voice assistants like Cortana, siri and Alexa are increasingly updating and are sounding more realistic.[7] A synthetic voice that sounds like a human raises several ethical concerns. As this technology can produce human-like voices, the probability is this synthetic voice technology is used to extort money from people by blackmailing them..
4) Affecting market - For defaming a product, tool, services, individual or a brand, deepfake technology can be easily used. This seems tough because a legal action or a suit can be filed only against a legal person. There are often fabricated online contents that can term certain products as harmful or poisonous made using the technology of deepfake. Mostly done by the rival companies to outpass the market competition. Most of the time, it is not possible to trace down the source of the content or verify the owner of the fake profile. Even if the source is traced down the act can be cleared by an alibi, it would most probably become too late and that might already have hampered the reputation.
Tracing the source - It is often seen that once these altered and fabricated videographic content or still images are shared online, it gets impossible to remove that from the social media platforms (internet). Often such kinds of contents go viral minutes after sharing and are shared, downloaded and uploaded multiple times. This gets

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

impossible for the respective authorities to bring the content down from online platforms and trace the IP address of the person who created and first shared or uploaded it.

**b) LEGAL CHALLENGES**

1) Manipulation of Evidence - Any evidence which is in the form of Audio - Visual form and is to be presented in the court has high chances of being altered with the use of deepfake technology, something that would be a roadblock to a truth and justice.[8] It possesses a challenge on our institutions' role in redefining the lines of evidences and truth in the process of providing justice in near future.
2) Liar's dividend - A new consequence is on the run, that is liar's dividend due to recent trend of media fact checking to address fake information. This phenomena includes debunking fake information not only provides it a longer lifetime but also actually legitimizes its existence and the debate over its accuracy. While thinking about mitigation strategies the effective role of liar's dividend is also needed to be considered.[9]Related to rules of evidence and truth, in short, the liar's dividend is the ability for deepfakes to sow enough doubt in public in the Audio Visual content,in large that people start claiming the real one as a deepfake content and fake one as the real content.
3) Consumer Protection - The deepfake generated social media filters raise privacy concerns over how the social media apps exploit user data in some instances.The viral Chinese Zao app, which allowed its users to swap their faces in their favourite movies and with the character they wanted to, by uploading their personal pictures. The terms of service of the app provided 'perpetual and transferable rights to the data uploaded', which raised major privacy concerns causing WeChat to ban the face swapping app Zao generated content.[10]

4) Privacy - The concern over the right to privacy being in danger due to the content being published using deepfakes because that covers non consensual manipulation, embellishment and distortion, as well as duplicitous uses of non-manipulated and original videographic content or still images for illustrative purposes.[11] The debate of privacy here arises over the use of celebrity faces as well as faces of ordinary people in non consensual pornography content. Sometimes it is often argued that an audio visual content shared publicly becomes private when manipulated.[12]
5) Political and personal freedom - Despiteful bots that are capable of producing fake news and social media content faster than any human writer, are behind the chaos caused in online media platforms.The role of deepfakes in creating and spreading wrong information and fake news challenges the main concept of fair and free elections. That creates a threat against violating the right to political participation and personal freedom.
Just like how people can easily use AI-powered deepfake technology to encourage the spread of fake information or are able to influence political public debate, they can easily use it to create and propagate and spread fake content designed to incite war or any kind of violence that can affect human life as well as property with their malicious and evil intentions.[13]
6) Defamation - A deepfake content can have anything, which may be related to an altered or fabricated videographic content or a still image. For an example, a video of an individual speaking some private information about another individual and that information tends to be true or an individual with public importance saying things in a video which he is not supposed to and the creator of the content just wanted to publish the content for fun or any other reason. In the first case, the victim for defamation here is the one who's private information is out, whereas, in the second case the individual in the video is defamed as he has been presented in a way that harms and derogates his image and hence is the victim. It is a technology that if not regulated precisely can cause harm to individuals of any social strata.

**4. International Legislations Regulating Deepfakes**

- **USA** - The house of representatives in the USA introduced the "*Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to accountability act of 2019*" also known as *DEEP FAKES*

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

*Accountability Act* to regulate the use of Deepfakes. After considering the detrimental use of the technology. This Act was passed with intention to impose liability, either the liability being civil or criminal upon the person who tends to create or share deep fakes without proper disclaimer.

This Act also curbs the misinformation being spread in public during the elections. Whereas, the Act also imposes criminal liability to deep fake pornography creators.[14] The Act further makes it mandatory for the deepfakes to be watermarked for the purpose of identification.

President Trump, in December 2019, signed for USA's first federal law regulating deepfakes in two provisions that are, 5709 and 5724 as part of (NDA) *National Defense Authorization Act* for the Fiscal year of 2020.

Some of the states of America too has taken steps regulating this technology, that are such as -

- **CALIFORNIA** - *Assembly Bill 730*[15] was passed ahead of the 2020 election due to the growing concerns over how fake information as a result of deepfake content can sway and manipulate voters. Whereas, the *Amendment Bill 602*[16], allows the residents of California to sue, if they believe their image has been used for sexually explicit or pornographic content. This legislation also provides the victims to seek injunctive relief and recover the reasonable cost and fees of attorneys.

  AB 730 & 602 hereby states, *Assembly Bill No. 730*[17] prohibits distributing "with actual malice" materially deceptive audio or visual media showing a candidate for office within 60 days of an election, with the intent to injure the candidate's reputation or deceive a voter into voting for or against the candidate.

  Cal. Elec. Code § 20010(a) [18]. states"Materially deceptive audio or visual media" must:

  1. "Falsely appear to a reasonable person to be authentic"; and
  2. "Cause a reasonable person to have a fundamentally different understanding or impression of the expressive content" than if he or she had seen the unaltered content.[19]

  Whereas, *Assembly Bill No. 602*[20] shall provide a private right of action against any person who:

  1. Creates and intentionally discloses sexually explicit material if that person knows or reasonably should have known the depicted individual did not consent; or
  2. Intentionally discloses sexually explicit material that the person did not create if the person knows the depicted individual did not consent.[21]

- **TEXAS** - Texas was the first state in the USA to prohibit political deepfake videos or images , that can probably influence the elections and also be liable to harm the candidates running for public offices.[22]

  *Texas Senate Bill 751*[23] addresses deepfake influenced videos and images only for regulating under the State's election code, which further states that, "anyone who alters or fabricates a video with an intention to hamper or influence the outcome of an ongoing election shall be charged to pay a fine of $4000 punishablewith an imprisonment up to an extent of one year in the county jail.[24]

- **VIRGINIA** - Virginia is the first state in the USA, which had a law banning revenge porn since 2014. However, that law did not include the altered and fabricated images and videos under the revenge porn law. But, in July 2019 Virginia officially updated its law to include deepfake images and videos and images.

  *Section 18.2-386.2 of the Code of Virginia* has been amended and reenacted, hereby states that, the unlawful sharing or disseminating or sale of any videographic or still images of any person with an intention to harass, coerce, created by any means, which includes altered or fabricated content (videographic or still images) that portrays another person, who is in a undressed state in such a manner that exposes the private parts where the creator of such content has a reason to know that he is not authorized to unlawfully disseminate or sell such content is liable of a Class 1 misdemeanor and shall be further punishable by an imprisonment of one year and fine upto $2500.[25]

- **CANADA** - Currently, Canada does not have any laws that criminalises the dissemination of fabricated or altered videographic content or still images online. However, the *Canada Elections Act* and the Criminal Code may regulate deepfakes.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

*Section 481(1)* of the *Canada Elections Act* states that, an offence of publishing any material *'regardless of its form'* that tends to be distributed during elections by any political party candidate.[26]As this section applies to any material, regardless of its form, there is a possibility of the same applying to the intentional online dissemination of fabricated video graphic content or still images.

Whereas, Section 162.1 of the Criminal Code, which regulates the prohibition of non-consensual pornography. This Section penalizes the publishing, distributing,transmitting, selling or advertising of an obscene image of an individual, knowing that he did not consent to that conduct. Also, this section does not require any sort of criminal intent or motive (mens rea).[27]

- **UK** - Currently there are no laws that regulates deepfakes particularly, but there are existing laws that can be applied. *The Defamation Act, 2013*[28] shall punish any published videographic content or still image which shall contribute in damaging an individual's reputation. According to the Act, the content published must cause some sort of 'serious harm' to the individual concerned in order to be actionable. The privacy laws such as, the Data protection Act 2018 and the laws under the (GDPR) *General Data Protection Regulation, Regulation 2016*[29] can also be applied to regulate deepfakes. It can be considered that most often deepfakes are generated using the data (images or videos) made available by sharing selfies, portrait pictures or videos on social media platforms by the concerned victims. Furthermore the deepfake content generated by using the original content shall look realistic.

  Nevertheless, if the deepfake content generated contains any confidential or private details, such as private facts about an individual being spoken by a deepfaked person. That shall be liable under the torts concerning breach of confidence and misuse of private information.

  As for revenge porn, the concerned regulators are considering updating and reenacting the existing laws with respect to clicking or taking, making and disseminating obscene or intimate images without consent. This however covers under the *Section 33 of Criminal Justice and Courts Act, 2015*[30], followed by the Voyeurism offences under the *Section 67 of the Sexual Offences Act, 2003*[31].

## 5. POSITION OF INDIA IN TACKLING CRIMES RELATED TO DEEPFAKE

India too has witnessed recent incidents related to deepfake revenge porn and deepfake technology being used in political campaigns. One was an incident in October 2019, where a man in Mumbai was arrested for an act of making a revenge deepfake porn video of his girlfriend just to threaten her.[32] Followed by in early months of 2020, in February two videos of Manoj Tiwari were released by BJP, where there was only one video but in two languages with an intention to reach two different linguistic voters.[33]

The achievable solution right now to tackle the upcoming threat of this technology is to combine the technology and the legislation. The recent trend of using this deepfake technology in making fake pornographic videos and political campaigns do raise several questions over the concerns related to privacy, identity theft and as well as the reality and authenticity of elections and the content available in social media platforms.

There is no law that directly deals with deep fakes. There can be several causes of action already existing in our existing laws and can be extended as well to cover the deepfake crimes. Some of the provisions are as follows -

1) **Defamation -** A person can be held liable for the act of defamation under the criminal as well as the civil law in India.[34] Also cyber defamation was earlier addressed under *Section 66A of IT*[35] Act. In civil law, defamation is punishable under the law of torts, where if the act is instituted and the act of defamation is found to be committed, damages shall be payable to the defamed person.[36] whereas, under the Indian criminal law, in *section 499 of IPC, 1860*[37] defamation is bailable, non-cognizable offence and compoundable offence and includes the publishing of some information that tends to cause some sort of harm to the reputation of the person. Punishment for the same has been provided under the *Section 500 of IPC, 1860*[38] which provides a sentence of imprisonment for up to two years or fine or both of these two.These laws are still not mature enough to deal with the various forms of existing deepfakes. Earlier cyber law too dealt with cyber defamation that was enshrined under *Section 66A of IT*[39] Act. The provision strictly covered any offensive information being sent by any computer source, with the intent of causing obstruction, insult, injury, hatred, criminal intimidation or ill

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

will. This provision no longer exists in the IT Act, and hence was struck down by the Supreme Court in the case of *Shreya Singhal v. Union of India.*[40]

2) **Right to Privacy** -

In the case of *Justice K. S. Puttaswamy v. Union of India*,[41] The nine judge bench recognised that a fundamental right to privacy is a fundamental right that is being protected under Part III of the Constitution of India, focused on the individual's right against the State and non-state actors for violations of their informational privacy, that recognizes an individual's control over his personal and digital privacy. This judgement was given in response to the argument of the AGI, where he considered that the Constitution of India does not include fundamental right to privacy with its connection to the legal challenge to Aadhaar Card (India's national identity project). Hence, using private or personal information like images, video clips in creating non consensual deepfake content of an individual shall institute violation of fundamental right to privacy.

Further, *Section 66E of IT Act, 2000* provides punishment for the violation of fundamental right to privacy if the accused person clicks or captures or publishes or transmits an image of a private area of any person without that person's express or implied consent, and does that knowingly or intentionally shall face imprisonment till three years or fine not exceeding the amount of two lakh rupees, or with both.

3) **Offences related to computers** -

The misuse of deepfake technology and the contents related to that in the web are nonetheless offences to be covered under IT Act, 2000 as it is also a computer related offence. The publication of obscene data in an electronic form is duly punishable under Section *67 of the IT Act, 2000*.[42] *Section 67A of the IT Act,2000* whereas also includes punishment for publishing content containing sexually explicit visuals in an electronic form.[43] Followed by, if the published material depicts children in sexually explicit form in an electronic platform shall be punishable under the Section 6*7B of IT Act, 2000*. If the deepfake content involves using any kind of unique identification feature, such as electronic passwords of an individual in a fraudulent manner, the accused person shall be punishable for the offence of, under the provided *Section 66C of IT Act, 2000*.[44]Furthermore, *66D of the IT Act, 2000* punishes for cheating by personation by using any computer resource.[45]

The Central Government, however, possesses the power to direct the intermediary to block any such deepfake content, if it finds necessary to do so, in the interest of protecting the sovereignty and integrity of India, national security, retaining friendly relations with the foreign states or to maintain public peace and order.[46]

4) **Copyright Infringement** -

Sometimes deepfake contents include altered versions of the sound and visual effects from a music video or a movie, which might be a copyrighted work. Section 14 of the Copyright Act, 1957 provides that the owner of that cinematographed music video or movie possesses exclusive right to license for making another copy of that film, including any picture or photograph of any image or any sound embodying it.[47] in the case of Amarnath Sehgal v. Union of India[48], Delhi High Court, the moral right of the author was recognised. The author cna claim damages for the act of mutilation, distortion or any sort of modification that would be prejudicial to his honour and responsible for causing a violation of his moral right over his creation.[49] The Copyright owner is liable to receive civil remedies by way of injunction, damages and otherwise may be conferred by law for infringement of the moral right over his licensed work.[50] Furthermore, if any person who deliberately abets the violation of the copyrighted work or any other rights conferred to the copyright owner under the ambit of the Act shall be punishable with imprisonment that may extend till three years and fine with which shall extend to the amount of two lakh rupees.[51] But these remedies might not work for the victim of a deepfake content, because generally it is seen that copyright is owned by the producers of the movies, not the actors, who hold up the risks of being a target and same applies for the pictures and photographs, the copyright would be owned by the photographer not by the person in the photograph. So, the remedies provided under this act might not be advantageous for the actual victim or the target of the deepfake content.

5) **Other Criminal Offences** -

The deepfake content can also be put under the radar of Section 468 of IPC, which defines the act of forgery, as the deepfake videos are generally the forged or copied versions of the original work and shall be liable to

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

constitute the offense of forgery and which is created with an intent to harm the reputation or image of any party knowingly shall be punished with a sentence of imprisonment of either for aterm extended till three years and also shall be liable to fine.[52] Section 124 of IPC, 1860 applies for the punishment of an act, where a deepfake content is liable to spread hatred or contempt or excite disaffection towards the Government of India. It shall be liable to punishment under the offence of sedition.[53]

Moreover Section 506 of IPC provides punishment for committing an offence in which there is a use of videos or images which threatens or intimidates any person or any of his property or his reputation.[54] Followed by the deepfake contents that tends to provoke breach of public peace and order[55], promoting communal outrage, promoting enmity between two religious or linguistic groups on the ground of caste, religion, race, language, place of birth or malicious acts to hurt religious feelings by insulting religious beliefs.[56]

6) **Data protection under the Personal Data protection Bill, 2019 (PDP Bill)** -

The legislature has introduced this bill with its aim to protect the privacy and data of an individual, so that by no means a personal data and privacy can be invaded without the consent of the data holder for processing of the personal data. The personal data includes one's image. The remedy for the violation of the rights protected under the act is right to be forgotten, which can be claimed against data fiduciary. The Bill is still not an Act yet. Moreover the right to be forgotten has already been recognised by some of the High Courts, such as Delhi, Kerala and Karnataka.[57]

## 6. Conclusion

Deepfake non consensual contents make it really accessible to fabricate or alter a media by using the face of an individual which in return has the potential to cause psychological harm, national security, market disruption, political instability etc.

Technology is developing day-by-day. Everyday there is some new addition in the aspect of technology. However, law does not develop at such pace and the present laws in India and several other countries don't have any legislation primarily regulating the deepfakes. The existing laws might not be sufficient to address the deepfake issues using technological algorithms. There might arise some issues on regulating deepfakes, such as[58]:

- Recognition and identification of deepfakes in real time.
- Attribution can be proved and culprits be punished.
- Acknowledging the gap in recognising if the content published supports the notion of freedom of speech or violates one's right to privacy.
- Ensuring that benefits for the victims is not outweighed while going through these lawsuits.
- The effect of the inherent rhythm of the courts, that needs to be restored in accordance with the current need of controlling and mitigating the effects of deepfakes.
- If the police departments are well equipped and trained to conduct investigations relating to deepfake contents.
- Technical knowledge that the legal attorneys must possess to conduct these types of criminal accusations.
- Removal of the deepfake content from the internet as early as possible.

These issues are long debated in the context of cybersecurity.

But we as a society, too, have a moral obligation to help curb the spread of non consensus malicious content. Educating ourselves and spreading awareness regarding the manipulations and the harm it can cause. Youth should be taught regarding the consequences of creating, uploading, downloading or sharing of fabricated content online. The regulators should look forward to adopting new methods in regulating the issues related to deepfakes, so that the source of the content is identified and blocked accordingly. 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 Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

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 public.[59]

The world has however started taking cognizance of the threat it possesses and this can be easily seen by several Countries looking forward to bringing this technology under their legal ambit. Regulating the big social media platforms is necessary so that they keep a check and balance on the fake content that is uploaded, shared and downloaded using their platforms that is capable of causing potential damages.

---

1Westerlund, Mika. . *The Emergence of Deepfake Technology: A Review*. Technology Innovation Management Review. 9. 39-52, (2019) https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_Technology_A_Review.
2JM Porup, *How and why deepfake videos work — and what is at risk*, CSO INDIA, (10 April, 2019 15:30 PM) ,https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html.
3 Raina Davis, Chris Wiggins, Joan Donovan, Deepfakes, SPRING 2020 SERIES, Rev, 1, (2020) https://www.belfercenter.org/sites/default/files/files/publication/Deepfakes_2.pdf .

4 Westerlund, Mika. . The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review. 9. 39-52, (2019). https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_Technology_A_Review
5 ibid.
6 John Bateman, *Get Ready for Deepfakes to be Used in Financial Scams*, CARNEGIE FORUM FOR INTERNATIONAL PEACE, (Aug 10, 2020) https://carnegieendowment.org/2020/08/10/get-ready-for-deepfakes-to-be-used-in-financial-scams-pub-82469#:~:text=of%20digital%20impersonation.-,The%20next%20big%20financial%20crime%20might%20involve%20deepfakes%E2%80%94video%20or,false%20depictions%20of%20real%20people.
7 Natasha Lomas, "*Duplex shows Google failing at ethical and creative AI design*",TECH CRUNCH, (May 10, 2018, 1:57 AM).https://techcrunch.com/2018/05/10/duplex-shows-google-failing-at-ethical-and-creative-ai-design/
8 Britt Paris, Joan Donovan, *Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence*, DATA SOCIETY, (2019). https://datasociety.net/wp-content/uploads/2019/09/DataSociety_Deepfakes_Cheap_Fakes.pdf .
9 Paul Chadwickl. *The Liar's Dividend, and Other Challenges of Deep-Fake News*, THE GUARDIAN. GUARDIAN NEWS AND MEDIA (July 22, 2018, 19:00 BST). https://www.theguardian.com/commentisfree/2018/jul/22/deep-fake-news-donald-trump-vladimir-putin.
10 Grace Shao and Evelyn Chen, *The Chinese face-swapping app that went viral is taking the danger of 'deepfake' to the masses*, CNBC, (, Jan 17 20202:50 AM EST) https://www.cnbc.com/2019/09/04/chinese-face-swapping-app-zao-takes-dangers-of-deepfake-to-the-masses.html.
11 David Fink, Sarah Diamond, *Deepfakes: 2020 and Beyond*, LAW.COM, (Sep 03, 2020 at 03:28 PM) https://store.law.com/Registration/Login.aspx?mode=silent&source=https%3A%2F%2Fwww.law.com%2Ftherecorder%2F2020%2F09%2F03%2Fdeepfakes-2020-and-beyond%2F .
12 Clare McGlynn, Erika Rackley & Ruth Houghton, *Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse*, Fem Leg Stud 25. Rev.25, 46 (2017). https://doi.org/10.1007/s10691-017-9343-2
13 *Human rights in the age of Artificial Intelligence* , https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.
Cal. Elec. Code § 20010(a) (2020)
14 Drew Harwell, *Fake-Porn Videos Are Being Weaponized to Harass and Humiliate Women: 'Everybody Is a Potential Target*', WASH. POST (Dec. 30, 2018, 10:00 AM), https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-beingweaponized-harass-humiliate-women-everybody-is-potential-target/
15 Assembly Bill 730, California.
16 Assembly Bill 602, California.
17 Assembly Bill 730, California.
18 California Elections Code, § 20010(a) (2020).
19 California Elections Code, § 20010(a) (2020)
20 Assembly Bill 602, California.
21 Caifornia Civil Code § 1708.85(b) (2020).
22 Chuck Lindell, *800 New Laws Take Effect Sunday*, Glen Rose Reporter, (Aug 29, 2019 at 11:24 AM), https://www.yourglenrosetx.com/news/20190829/800-new-laws-take-effect-sunday-what-you-need-to-know
23 Texas Senate Bill 751.
24 Douglas Ketterman, *'Deepfake' Videos Under Spotlight of New Texas*, KRWLAWYERS.COM, (03 Jan, 2021, 09:54 AM)https://www.krwlawyers.com/blog/deepfake-videos-under-spotlight-of-new-texas-law/
25Code of Virginia. § 18.2-386.2, https://law.lis.virginia.gov/vacode/title18.2/chapter1/section18.2-11/
26 Canada Elections Act, SC 2000, C 9, s 481
27 Criminal Code, RSC 1985, c C-46, s 162.1(1)
28 Defamation Act, 2013, UK Public general Acts.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 2226 - 2235

29 The General Data Protection Regulations, Data Protection Act 2018, c. 12 Available at http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted .
30 Criminal Justice and Courts Act, 2015, Section 33.
31 Sexual Offences Act, 2003, Section 67.
32 Parth Tyagi and Achyutam Bhatnagar, *Deepfakes and the Indian legal landscape*, INFORM.ORG ,(July 03, 2020) https://inforrm.org/2020/07/03/deepfakes-and-the-indian-legal-landscape-parth-tyagi-and-achyutam-bhatnagar/
33 Nilesh Christopher, *We've Just Seen the First Use of Deepfakes in an Indian Election Campaign*, VICE.COM (Feb 02, 2020) https://www.vice.com/en_in/article/jgedjb/the-first-use-of-deepfakes-in-indian-election-by-bjp. ,
34 T. Pradeep & Aswasthy Rajan, *A Critical Study on Cyber Defamation and Liability of ISPS*, 119(17) International Journal of Pure and Applied Mathematics, 1717, 1719 (2018)https://acadpubl.eu/hub/2018-119-17/2/139.pdf .
35 Information & technology, 2000, Section 66A.
36Rashmi Senthilkumar, *Defamation law in India*, LEGALSERVICEINDIA.COM (Jan 05, 2021, 18:10 PM) http://www.legalserviceindia.com/legal/article-2224-defamation-law-in-india.html
37 Indian Penal Code, 1860, Section 499
38 Indian Penal Code, 1860, Section 500
39 Information & Technology Act, 2000, Section 66 A.
40 A.I.R. 2015 S.C. 1523.
41 (2017) 10 S.C.C. 1.
42 Information and Technology Act, 2000, Section 67.
43 Information and Technology Act, 2000, Section 67A.
44 Information & Technology Act, 2000, Section 66C
45 Information & Technology Act, 2000, Section 66D,

46 Information and Technology Act, 2000.Section 69A,
47 The Copyright Act, 1957.Section 14(d) and Section 14(e),
48 117 (2005) DLT 717.
49 Copyright Act, 1957.Section 57,
50 Copyright Act, 1957.Section 55,
51 Section 63, Copyright Act, 1957.
52Indian Penal Code, 1860, Section 469
53 Indian Penal Code 1860, Section 128
54 Indian Penal Code 1860, Section 506.
55 Indian Penal Code, 1860.Section 504.
56 Indian Penal Code 1860.Section 295A.
57 Parth Tyagi and Achyutam Bhatnagar, *Deepfakes and the Indian legal landscape*, INFORM.ORG ,(July 03, 2020) https://inforrm.org/2020/07/03/deepfakes-and-the-indian-legal-landscape-parth-tyagi-and-achyutam-bhatnagar/
58Vanessa Henri,International: Deepfakes and their risks to society, DATAGUIDANCE.COM https://www.dataguidance.com/opinion/international-deepfakes-and-their-risks-society
59Rajmohan, Ganga.. *Deepfakes and the Indian Law*. (2020) 10.13140/RG.2.2.16798.77128. https://www.researchgate.net/publication/345809619_DEEPFAKES_AND_THE_INDIAN_LAW
60Dhabliya, M. D. (2019). Uses and Purposes of Various Portland Cement Chemical in Construction Industry. Forest Chemicals Review, 06–10.
61Dhabliya, M. D. (2018). A Scientific Approach and Data Analysis of Chemicals used in Packed Juices. Forest Chemicals Review, 01–05.
62Dhabliya, D. (2021a). AODV Routing Protocol Implementation: Implications for Cybersecurity. In Intelligent and Reliable Engineering Systems (pp. 144–148). CRC Press.
63Dhabliya, D. (2021c). Designing a Routing Protocol towards Enhancing System Network Lifetime. In Intelligent and Reliable Engineering Systems (pp. 160–163). CRC Press.