Vol. 15 No. 1 ISSN: 0976-3570

Deepfakes on Copyright Law- Inadequacy of Present Laws in Determining the Real Issues

Aranya Nath[1]
Sreelakshmi B.[2]

Abstract

We are in the 21st century, where rapid development of deep fakes technology led to cause harmful consequences justifies some form of regulation. The proposed laws are diverse, addressing many hazards linked with deep fakes. Rather than exploring the field, this Article investigates solutions to a specific set of concerns relating to national security. The interests are concerned with challenges to our social order. A bad actor may use deep fakes to exploit societal differences, destabilize political discussion, and erode faith in political institutions. The ensuing concrete harms might have far-reaching consequences for campaign reform, military operations, and intelligence collection missions, among other things. This Article discusses the legal and constitutional restrictions on any law aiming at legislating deep fakes and the issues related to national security.

Keywords*: Deepfakes, Copyright. National security, WIPO, artificial Intelligence, Intellectual Property Law, Information Technology Law*

I. Introduction

Deepfake is a blend of deep learning and fake. It is a synthetic artificial intelligence used to generate pictures, audio, and video in which an actual person in the image, audio, or video is substituted by another individual using generative adversarial networks.[3] Deepfakes are media or digital representations altered via

[1] Ph.D Scholar Damodaram Sanjivayya National Law University, Visakhapatnam Andhra Pradesh, India.

[2] Research Assistant, The Centre for Research, Development and Training in Cyber Laws and Cyber Security, TNNLU. LLM Jindal Global University Haryana, BA LLB TNNLU.

[3]'A Beginner's Guide to Generative Adversarial Networks (GANs)' (*Pathmind*) <http://wiki.pathmind.com/generative-adversarial-network-gan> accessed 21 October 2022.

artificial intelligence and deep learning. It has been employed in various industries, including entertainment, medical technology, and education. Several organizations have utilized the technology for lawful reasons. It has been used in the medical field to teach artificial intelligence to identify tumours[4] and in the entertainment industry to make parodies and resuscitate deceased artists. [5]

Deepfakes rely on Auto-encoder, a neural network. An encoder converts a picture to a lower-dimensional subspace, while a decoder reconstructs the image from the latent representation. This architecture uses a universal encoder that encodes a person into the latent space. The hidden representation includes essential information about their facial characteristics and body position. It decrypts using a model trained exceptionally for the target. It will place the target's comprehensive information on the original video's underlying face and body features, represented in the latent space. So, it is prominent that the deep fakes create for malicious purposes like harassment of women in the form of vengeance porn[6] and post-truth politics.[7]

The legal implications of using deep fake content have been widely debated across various jurisdictions as they impact laws relating to copyright, defamation, and the threat to national security and privacy using artificial intelligence. Therefore, it states a few hazards associated with Deepfakes as privacy is recognized as a fundamental right under article 21 of the Indian Constitution. However, the fact is that PDP is not an act still now, so under copyright right to be forgotten has been taken in the recent past because social media platforms are

[4] Jackie Snow, 'Deepfakes for Good: Why Researchers Are Using AI to Fake Health Data' (*Fast Company*, 24 September 2018) <https://www.fastcompany.com/90240746/deepfakes-for-good-why-researchers-are-using-ai-for-synthetic-health-data> accessed 21 October 2022.

[5] 'This Iconic Filmstar Will Star in a New Movie - from beyond the Grave' (*World Economic Forum*) <https://www.weforum.org/agenda/2019/11/james-dean-cgi-deepfakes/> accessed 21 October 2022.

[6] 'Mapping the Deepfake Landscape · Giorgio Patrini' <https://giorgiop.github.io/posts/2018/03/17/mapping-the-deepfake-landscape/> accessed 21 October 2022.

[7] 'Why the Manoj Tiwari Deepfakes Should Have India Deeply Worried' <https://theprint.in/tech/why-the-manoj-tiwari-deepfakes-should-have-india-deeply-worried/372389/> accessed 21 October 2022.

ill-equipped to deal with them due to the lack of requisite technology to detect them.

II. Deep Fakes Technology: An Overview

Artificial intelligence (AI) programs that merge mix, replace, and superimpose photos and video clips to create fake videos that look real are known as deep fakes. In 2014, Ian Goodfellow made it. Even without the user's consent or permission, they could use deepfake technology to create, for instance, a humorous, pornographic, or controversial film of a person speaking. As users tend to stick with the group, deepfakes target social media platforms where conspiracies, rumours, and false information may spread quickly.[8]

A. The Creation of Deep Fake Technology

Academic researchers and computer graphics studios have already pushed the capabilities of video and picture manipulation. However, deepfakes were first created in 2017 when a Reddit user with a similar moniker posted edited videos. A face-swap video is made in a few steps. The two people's hundreds of facial images are first put through an encoder, an AI algorithm. The encoder identifies & remembers similarities among the two faces, reducing them to their shared characteristics, and compresses the images. Such features are then trained to be recovered first from compressed photos by a second AI system known as a decoder.

A generative adversarial network, or GAN, is another technique for creating deepfakes. Two AI algorithms are pitted against one another in a GAN. The generator, the main algorithm, receives random noise and generates an image from it. Then, a set of real photographs are given to the discriminator, the second algorithm, and this synthetic image. The artificial pictures will not initially resemble faces at all. However, the discriminator and generator both advance by repeatedly using the strategy and receiving constructive feedback. If the generator gets sufficient input and loops, it will begin to produce compelling features of wholly fictitious superstars.

[8] Hrisha Yagnik, Akshit Kurani and Prakruti Joshi, 'A Brief Study on Deepfakes' (2020) 07 5.

B. Deepfakes Require Specialized Technology.

On a regular computer, it is challenging to generate an accurate deepfake. Most produce cutting-edge desktop computers with potent graphics cards or, even better, cloud computational power. The period is shortened from days and weeks to hours. However, it also requires skill to edit finished films to reduce flicker and other aesthetic flaws. A variety of tools are now accessible to help users create deepfakes. Many businesses will make them for you (deepfakesweb.com), and the cloud will conduct all the processing. There is also a smartphone application called Zao that allows users to layer their features to various TV and movie personalities that the system has been taught to recognize.

III. Harmful Threats of Deep Fakes

Understanding the underlying harms and their potential effects is necessary to appropriately address the threat posed by deepfakes. It should consider the views of prominent individuals in science, technology, and government.[9] The initial phase in developing a concentrated legal solution recognizes the underlying harms and how deepfakes impact their viewers.

A. National Security Threats

Deepfakes pose severe concerns to our national security when used by unscrupulous actors. The rapid adoption of technology that makes it possible to create deepfakes has also sparked worries among lawmakers. Those who have questioned the Director of National Intelligence to assess threats to national security claimed that they could use such technology to spread disinformation, take advantage of social tensions, and foment political unrest. [10]

Deepfakes' ability to distribute false information might endanger national security. For instance, if a deepfake shows military personnel criticizing, attacking, or killing civilians, it might threaten the safety of military forces

[9] ‘Deepfakes Will Influence the 2020 Election’ <https://qz.com/1660737/deepfakes-will-influence-the-2020-election> accessed 22 October 2022.

[10] Schiff, Murphy, and Curbelo Request DNI Assess National Security Threats of “Deep Fakes,” https://schiff.house.gov/news/press-releases/schiff-murphy-and-curbelo-request-dni-assess-national-security-threats-of-deep-fakes (last visited Oct 22, 2022).

interacting with foreign civilians in danger.[11] A bad actor might employ a deepfake to incite the local community by exploiting the unrest in the area. It could result in civilian fatalities, increased enemy recruiting, or violent clashes with American forces.[12]

Hostile foreign governments may use Deepfakes to fabricate propaganda showing world leaders shouting harsh language or ordering crimes.[13] Thus, due to their persuasive power, aided by the dissemination capabilities of social networking sites, hyper-realistic deepfakes represent a distinct threat to public safety and national security. [14]

If deepfakes are used to deceit during the war, it could threaten national security.[15] Here, malicious actors may masquerade as military or intelligence personnel to direct the transfer of sensitive material or take another action that would expose forces to vulnerability.[16] A deepfake might be extensively circulated and endanger an entire governmental regime or national economy when combined with a cyberattack, such as a breach of a news organization's website or a cache of official data.[17] An opponent may, for instance, get private papers and selectively release deep-fake forgeries alongside the originals. Governmental officials would also encounter great difficulties restricting and remediating the potentially severe implications of a fraudulent document release after actual or fake papers disseminates.

[11] '"Deep Fakes: A Looming Challenge for Privacy, Democracy, and National S" by Danielle K. Citron and Robert Chesney' <https://scholarship.law.bu.edu/faculty_scholarship/640/> accessed 22 October 2022.

[12] '"Deep Fakes: A Looming Challenge for Privacy, Democracy, and National S" by Danielle K. Citron and Robert Chesney' (n 11).

[13] 'Allen and Chan - 2017 - Artificial Intelligence and National Security.Pdf' <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf> accessed 22 October 2022.

[14] '"Deep Fakes: A Looming Challenge for Privacy, Democracy, and National S" by Danielle K. Citron and Robert Chesney' (n 11).

[15] Schiff, Murphy, and Curbelo Request DNI Assess National Security Threats of "Deep Fakes," *supra* note 10.

[16] 'Allen and Chan - 2017 - Artificial Intelligence and National Security.Pdf' (n 13).

[17] 'Allen and Chan - 2017 - Artificial Intelligence and National Security.Pdf' (n 13).

B. Political Threats

Political misinformation: The world has experienced numerous actions at fake videos featuring a politician or public officer speaking his mind and the video going viral on social media sites with the malignant intention of causing distress and spreading false information like fires among the people. Fake political news developed with deepfake technology poses a threat to civilization. Facebook and other social networking sites have been under continual pressure to remove deepfake information from their platforms. In 2018, for example, a fake film showing Obama criticizing Donald Trump was circulated.

Political satire: Occasionally, a deepfake video is created with a politician's body and facial features but also with a different and fake speech, with fake speech usually extraordinarily light and amusing.

In that situation, the goal of the material is to elevate the social message underlying the satire rather than to propagate false information. Social media companies such as Facebook have been spotted attempting to discern between deepfakes distributing incorrect information and deepfakes created for satire.

Deep Fake News: The media profession may suffer as a result of its failure to saturate fake and authentic material before transmitting it to its consumers. Traditional fake news poses a lower danger than deepfakes since they are more challenging to identify, and people believe what they see as accurate. The technology can make seemingly credible news films that harm the news agency's image.

In today's world, a racial group that offers news to its viewers and access to video evidence fired by a witness of an incident can provide a competitive advantage to a news agency. As a result, to be the first in the race, they frequently miss out on verifying if the footage is real or fake.[18]

C. Pornographic Threat

The negative aspect of deepfakes, especially non-consensual and revenge porn, is that this technology allows the utilization of public information faces in the

[18] Mika Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 40.

pornographic video without their agreement. Celebrities are frequently victims of non-consensual porn generated with deepfake technology.

Deepfake revenge porn can violate victims' rights to their pictures and privacy, which is a big problem. Deepfake pornographic videos of celebrities and celebrities falling victim to such videos are frequently heard. Still, these videos are increasingly being utilized against regular men, women, and children. Deepfake porn movies featuring ordinary people are now being released solely to ridicule them. [19]

IV. Regulation of DeepFakes: Scope of the Present Regulations

The threats and concerns posed by deepfakes makes it necessary that it be regulated. In order to determine the regulatory framework for deepfakes, there is need into look into the primary stakeholders involved in deepfakes. It can be observed that generally there are four stakeholders involved in deepfakes. The major stakeholders related to deepfakes are: deepfake persons, deepfake makers, deepfake viewers and deepfake disseminators. [20] Deepfake person refers to the individual whose information was used to create the Deepfake; Deepfake maker refers to the individual who created the Deepfake; Deepfake viewer refers to the individual who received or viewed the Deepfake; and Deepfake disseminator refers to the individual offering means to propagate the Deepfake such as distributors, internet service providers, or other intermediates.[21] It is necessary to regulate deepfake considering the above key stakeholders. A deepfake individual's right to privacy, data protection rights, right of publicity, copyright, etc., could all be infringed upon by deepfake content. Therefore, the law must be able to safeguard the deepfake individual from having any of their rights violated. Deepfake maker has his right to freedom of speech and expression which is not

[19] 'Deepfake Videos Being Used to Blackmail People' <https://www.komando.com/security-privacy/deepfake-porn-videos-are-now-being-used-to-publicly-harass-ordinary-people/526877/> accessed 23 October 2022.

[20] 'Rebalancing Our Regulatory Response to Deepfakes with Performers' Rights - Mathilde Pavis, 2021' <https://journals.sagepub.com/doi/full/10.1177/13548565211033418> accessed 4 November 2022.

[21] 'Rebalancing Our Regulatory Response to Deepfakes with Performers' Rights - Mathilde Pavis, 2021' (n 20).

absolute and if the deepfake content is infringing or violating the right of the deepfake person or deepfake viewers which and comes under the reasonable restriction, then the law should be able to regulate this. Deepfake viewer has the right to information which should not be curtailed by way of deepfake content and thus regulation should consider this aspect as well. Deepfake disseminators like the intermediaries should also be regulated so that they can be a vehicle of freedom of expression but should not be the reason behind the violation of rights of the deepfake person or deepfake viewer. Thus, the rights of these stakeholders need to be balanced. As deepfake content is not always harmful and can be beneficial, a blanket ban of deepfake can thus go against the rights of stakeholders.

There is not yet a criminal statute or civil liability regime in place that makes it illegal to create or distribute deepfakes.[22] It is pertinent to note that there is no exclusive regulation to deal with the ethical, socio-political, or legal issues posed by deepfakes, and that the existing laws only cover piecemeal protection of certain aspects. When deepfakes are considered, issues pertaining to intellectual property law, tort law, criminal law, and civil law all come into play. Some of the legal remedies that can be used by a deepfake persons are: right to privacy, tort of breach of confidence, passing off, defamation, malicious falsehood, copyright, performers right, data protection, civil and criminal remedies.[23]

There is gap in the existing laws to regulate the harms posed by deepfakes. Deepfake content is not necessarily be related with living persons. In case of deepfake content relating to a dead person, the remedies such as right of privacy, malicious falsehood and defamation cannot be availed as these rights are not recognized posthumously, especially in the common law countries.[24] Legal remedies that are currently available do not apply effectively, and in some cases do not apply at all, to unauthorized uses of material that has been lawfully made

[22] '"Deep Fakes: A Looming Challenge for Privacy, Democracy, and National S" by Danielle K. Citron and Robert Chesney' (n 11).

[23] 'Rebalancing Our Regulatory Response to Deepfakes with Performers' Rights - Mathilde Pavis, 2021' (n 20).

[24] Dr Bo Zhao, 'Posthumous Reputation and Posthumous Privacy in China: The Dead, the Law, and Social Transition' 39 85.

public in the past, or that is related to public persons.[25] The remedy of passing off can only be claimed by deepfake individuals who possess the one of the classical trinities of passing off,[26] goodwill or reputation. Thus, the scope of the passing off remedy of a deepfake person is limited.[27] Similar, in claims like malicious false hood, defamation and passing off, there is requirement to show significant harm which also restricts the scope of using these remedies even when the deepfake person's data is used.[28] When a deepfake maker's identity is unknown or their actions have been concealed, the deepfake person's ability to bring or pursue legal action against them is severely hampered, if not entirely defeated. This obstacle is due to the difficulty of the deepfake individuals to attribute the harm caused to them by the deepfake maker. When this happens, deepfake individuals may be left with no choice but to seek redress from the platform owners who allowed the content to be widely disseminated.[29] In case of copyright and defamation, by way of take-down notice to the disseminator, the infringing deepfake content can be asked to be removed. The subject of a copyright need not be the same person who owns the copyright, and if the subject is a deepfake person, then he has no recourse under copyright law.[30] The right of the deepfake person, who is also the data subject, can be protected using the data protection that is guaranteed by the EU General Data Protection

[25] 'Rebalancing Our Regulatory Response to Deepfakes with Performers' Rights - Mathilde Pavis, 2021' (n 20).

[26] 'Passing Off: The Jif Lemon Case (Reckitt & Colman Ltd v Borden Inc) - Tanner De Witt' (*Tanner De Witt Solicitors, Law Firm Hong Kong*) <https://www.tannerdewitt.com/passing-off-the-jif-lemon-case-reckitt-colman-ltd-v-borden-inc/> accessed 4 November 2022.

[27] Andrew Ray, 'Disinformation, Deepfakes and Democracies: The Need for Legislative Reform' (2021) 44 University of New South Wales Law Journal <https://www.unswlawjournal.unsw.edu.au/article/disinformation-deepfakes-and-democracies-the-need-for-legislative-reform/> accessed 4 November 2022.

[28] 'Rebalancing Our Regulatory Response to Deepfakes with Performers' Rights - Mathilde Pavis, 2021' (n 20).

[29] '"Deep Fakes: A Looming Challenge for Privacy, Democracy, and National S" by Danielle K. Citron and Robert Chesney' (n 11).

[30] 'Rebalancing Our Regulatory Response to Deepfakes with Performers' Rights - Mathilde Pavis, 2021' (n 20).

Regulation.[31] Only certain legal jurisdictions offer this remedy, which is one of the most significant drawbacks. This is because harmonized data protection regulation does not yet exist. This is also the case with other remedies, as the level of protection offered by the legal remedies that can be obtained for deepfake content may be lesser, or there may be no protection at all. Therefore, the use of data across international borders has a significant gap due to the absence of universal harmonization.[32] Although there are restrictions of legal liability in many other contexts, the fact that internet platforms are accessible all over the world makes this a particularly challenging issue in the case of deep fakes.[33]

Therefore, as technology and AI continue to advance, there will be a greater need to amend existing legislation to stay up with technology and avoid the misuse of deepfake technology. One of the major challenges in regulating deepfakes is to make sure that the freedom of expression is not taken away. Deepfakes has its own advantages and especially in areas like education deepfake technology will have benefits. A regulation that put on outright ban of deepfake is not the solution and regulations have to be made trying to balance the freedom of expression with that of the harms posed by deepfakes. Therefore, the regulation should not be too broad to effectively impede deepfake's potential benefits.

V. Indian Scenario

While neither civil nor criminal law in India currently mentions deepfakes, a review of a few of the existing laws and regulations reveals the possibility of adapting such laws to address issues concerning deepfakes and to what extend deepfake contents are permitted.

[31] 'Regulation 2016/679 - Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) - EU Monitor' <https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk3t7p3lbczq> accessed 1 August 2022.

[32] 'Rebalancing Our Regulatory Response to Deepfakes with Performers' Rights - Mathilde Pavis, 2021' (n 20).

[33] '"Deep Fakes: A Looming Challenge for Privacy, Democracy, and National S" by Danielle K. Citron and Robert Chesney' (n 11).

A. Constitutional provisions

The scope of privacy protections in India has expanded as a result of the ruling on the Right to Privacy in *Justice K.S. Puttaswamy v. Union of India*.[34] The 9 judges bench unanimously declared right to privacy as a fundamental right under Article 21. Since digital privacy is a subset of informational privacy, the use of private information in deepfake videos, such as photos or audio-visual clips, without the consent of the subject would be a violation of his or her fundamental right to privacy in the Indian context.[35]

Despite being false, one of the reasons why there cannot be outright ban on deepfakes is the fact that it will be infringing freedom of speech and expression as guaranteed under Article 19(1) (a). However, since this is not an absolute right and comes under reasonable restriction, deepfakes that is infringing other legal rights can be regulated.

B. Provisions under Information Technology Act

The Information Technology Act, 2000 the first cyberlaw in India with the aim of regulating cyberspace have provisions to deal with cybercrimes. However, due to the non-comprehensive nature of coverage of cybercrimes under IT Act, 2000, the Act alone does not have the capacity to regulate deepfakes. Some provisions of IT Act that can be invoked to deal with deepfakes are explained below.

Under the IT Act, computer-related offences can be committed if deepfakes are used inappropriately or abused. Section 67 of the Act provides for penalties for the electronic publication or transmission of obscene material and if the deepfake created is obscene then it would attract this provision.[36] Section 67A of the Act outlines the penalties for publishing or transmitting material in electronic form that contains sexually explicit act or conduct and thus a deepfake which contain

[34] Justice K.S. Puttaswamy (Retd) ... vs Union Of India And Ors. on 24 August, 2017, https://indiankanoon.org/doc/91938676/ (last visited Oct 31, 2022).

[35] 'Puttaswamy v. Union of India (I)' (*Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/> accessed 10 November 2022.

[36] Cyber Lawyer, 'Section 67 of Information Technology Act: Punishment for Publishing or Transmitting Obscene Material in Electronic Form' (*Info. Technology Law*, 18 September 2014) <https://www.itlaw.in/section-67-punishment-for-publishing-or-transmitting-obscene-material-in-electronic-form/> accessed 10 November 2022.

sexually explicit act will attract penalties. Section 67B of the Act criminalizes the publication or transmission of material in electronic form that depicts children engaging in sexually explicit act or conduct and will apply to deepfakes involving children. The deepfake maker shall be punishable for the offence, under the provided Section 66C of IT Act, 2000, if the deepfake content uses any kind of unique identification feature, such as electronic passwords, of a person in a fraudulent manner. This includes using the identity of a foreign state or public peace and order. In addition, section 66D [37]of the Act penalizes the use of a computer to commit fraud through impersonation. By virtue of Section 69A,[38] the Central Government has the authority to direct the intermediary to block any such deepfake content if it determines that doing so is necessary for the purposes of preserving the independence and territorial integrity of India, maintaining India's national security, and fostering cordial relations with other nations.

Apart from computer related offence, IT Act provides penalties for violation of right to privacy. Section 66E of the Act outlines the penalties for violating a person's right to privacy as follows: if the accused person intentionally or knowingly photographs, publishes, or transmits an image of a private area of another person without that person's consent, the accused person is subject to a sentence of imprisonment of up to three years or a fine of up to two lakh rupees, or both, depending on the severity of the offence.[39]

Another provision in IT Act that deal exclusively with cyber defamation is Section 66A. Sending any information via a computer resource that is excessively offensive or has a menacing nature; or is for the purpose of creating annoyance, discomfort, danger, obstruction, insult, injury, criminal intimidation, hostility, hatred, or ill will is punishable by this section. However, the Apex Court

[37] 'Section 66D of Information Technology Act: Punishment for Cheating by Personation by Using Computer Resource, Facebook, Fake Profile' <https://www.itlaw.in/section-66d-punishment-for-cheating-by-personation-by-using-computer-resource/> accessed 10 November 2022.

[38] 'Section 69A in The Information Technology Act, 2000' <https://indiankanoon.org/doc/10190353/> accessed 10 November 2022.

[39] 'India Code: Section Details' <https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=81> accessed 10 November 2022.

in *Shreya Singhal v. Union of India*[40] nullified this section of the IT Act, making it obsolete. Thus, this provision holds no value in addressing deepfakes.

The previous provisions were mainly to deal with deepfake makers. The IT Act also provides for the liabilities of intermediaries. Since intermediary's host deepfake content, Section 79 of the Act regulates their liability. After discovery or court order, the intermediary may remove the content. In *Myspace Inc. v Super Cassettes Industries Ltd.*,[41] the Court ruled that intermediaries must remove copyright-infringing information upon private party complaint without a Court order. Currently, intermediaries are only required to advise users about not posting certain kinds of harmful/unlawful content. The newly proposed IT rules draft however establish a legal requirement on intermediaries to take reasonable efforts to prevent users from posting such content. The new clause will ensure that the intermediary's obligation is not a mere formality.

C. Provisions under IPC

The provisions of the IPC, 1860 are duly invoked given the non-comprehensive nature of coverage of cybercrimes under IT Act, 2000.

Section 468 of the IPC defines forgery, and deepfake videos are usually faked or copied. As such, they are liable to constitute the offence of forgery, and content prepared with the intent to injure the reputation or image of any person deliberately is punished by a sentence of imprisonment of up to three years and a fine.[42] Section 124 of the IPC applies to deepfakes that encourage hatred or contempt for the Indian government and constitutes sedition.[43]

The offence of criminal intimidation as under Section 503 is also committed if the person in the deepfake video is threatened with injury to his reputation or the property of him or an interested party with the intent to frighten that person or

[40] 'Shreya Singhal vs U.O.I on 24 March, 2015' <https://indiankanoon.org/doc/110813550/> accessed 4 November 2022.

[41] 'My Space Inc. vs Super Cassettes Industries Ltd. on 23 December, 2016' <https://indiankanoon.org/doc/12972852/> accessed 4 November 2022.

[42] 'IPC Section 468 - Forgery for Purpose of Cheating' (*A Lawyers Reference*) <https://devgan.in/ipc/section/468/> accessed 10 November 2022.

[43] 'India Code: Section Details' <https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00037_186045_1523266765688&sectionId=45863&sectionno=124A&orderno=133> accessed 15 November 2022.

cause him or her to conduct or omit an illegal act. The use of photographs or moving images with the intent to menace or intimidate another person, his property, or his reputation is a crime punishable under Section 506 of the Indian Penal Code. Also, based on the likely effects of the content of the deepfake, the deepfake maker can be charged with the crime of intentional insult with the intent to cause a breach of the peace as under Section 504, promoting hatred between different groups based on religion, race, place of birth, residence, language, etc., and doing things that make it hard to keep the peace as under Section 153A, or for deliberate and malicious acts meant to hurt the religious feelings of any class by insulting its religion as under Section 295A.[44] If the deepfake content is a fake pornographic video that is be spread by the deepfake maker, then Section 354 can be charged for outraging the modesty of a women and sexual harassment under section 354A.[45] If an offensive deepfake photo is passed around, it would be against the law according to Section 292 of the IPC.[46] Section 499 of the IPC makes it clear that posting material with the intent to hurt someone's reputation constitutes defamation, which is a bailable, non-cognizable offence that can be compounded.[47] Section 500 of the IPC specifies as punishment for this offence imprisonment for up to two years or a fine, or both. These regulations are immature and cannot address the myriad of deepfakes already in existence.[48]

D. Provisions under Copyright Act

Deepfakes often feature modified copies of music videos or movies that contain elements that are protected by copyright laws. The owner of a cinematographed music video or movie has the sole right to license the making of any other copy

[44] 'Section 295A in The Indian Penal Code' <https://indiankanoon.org/doc/1803184/> accessed 15 November 2022.

[45] 'IPC Section 354 - Assault or Criminal Force to Woman with Intent to Outrage Her Modesty' (*A Lawyers Reference*) <https://devgan.in/ipc/section/354/> accessed 15 November 2022.

[46] 'Section 292 in The Indian Penal Code' <https://indiankanoon.org/doc/1704109/> accessed 15 November 2022.

[47] Diva Rai, 'Defamation: Section 499 to 502 of the Indian Penal Code' (*iPleaders*, 24 January 2020) <https://blog.ipleaders.in/defamation-section-499-to-502-of-ipc/> accessed 10 November 2022.

[48] 'IPC Section 500 - Punishment for Defamation' (*A Lawyers Reference*) <https://devgan.in/ipc/section/500/> accessed 10 November 2022.

of the film, including any picture or photograph of any image or any sound embodying it, according to Section 14 of the Copyright Act, 1957. Anybody violating the copyright of the copyright holder will be liable under Section 51 of the Act. Similarly, Section 57 of the Act provides for moral rights. Author's moral rights were upheld in the case *Amarnath Sehgal v. Union of India*,[49] heard in the Delhi High Court. If the author's work is mutilated, distorted, or otherwise changed in a way that brings shame on him or his work, the author has the right to sue for damages. In the event of an infringement of the Copyright owner's moral right over his licensed work, the Copyright owner is entitled to injunctive relief, damages, and any other relief that may be provided by law.[50] Additionally, anybody who knowingly aids in the infringement of a copyrighted work or any other rights granted to the copyright owner under the ambit of the Act shall be penalized with imprisonment that may extend up to three years and a fine that shall extend to the amount of two lakh rupees. However, these solutions may not help a victim of deepfake content if the copyright in question does not belong to the person who is depicted in the image in the case of movies, this would be the producers rather than the performers who bear the dangers of being a target. Therefore, the real victim or intended audience of the deepfake content may not benefit from the remedies allowed by this law. Another defence that can be taken in favor of deepfake is fair use defence under Section 52 of the Act. [51]

VI. Conclusion

Deep learning originated as a novel method with the development of artificial Intelligence, data science, and high-speed networks. Such deepfakes, like all other technology developments, have been used for illicit and unethical purposes. This deepfake technology can alter an economy's functioning, people's freedom,

[49] Janhavi KM, 'Amarnath Sehgal v. Union of India' (*IP Matters*, 22 August 2022) <https://www.theipmatters.com/post/amarnath-sehgal-v-union-of-india> accessed 10 November 2022.

[50] 'Protection of "Moral Rights of Author"' (*S.S Rana & Co*, 24 December 2021) <https://ssrana.in/articles/protection-moral-right-author/> accessed 10 November 2022.

[51] 'Applicability of Section 52 of the Copyrights Act to Specific Works - Lexology' <https://www.lexology.com/library/detail.aspx?g=6634c94d-77bf-40fb-8a56-e82da8067285> accessed 10 November 2022.

and a nation's security. Individuals must be aware of such technologies, and significant social media platform service providers should monitor such actions.

For safeguarding individual privacy, deepfakes technology needs to have a comprehensive set of rules and regulations. This technology not only has an impact on data infringement, but it may also negatively impact people's life. It is also worth noting that it may utilize this technology for good. People who use this technology should consider their work's ethical and societal implications. It is a well-known idea that everything has both good and negative consequences. We must collaborate to uncover more benefits of employing this technology.