Page 1119 - 1132

DOI: *https://doij.org/10.10000/IJLMH.116832*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 1

2024

Addressing Deepfake through the Existing Legal Strategies in Bangladesh: An Assessment

Md. Al-Amin Hossain[1]

Abstract

A camera, so the saying goes, cannot lie. However, it has become clearly evident in this digital age that it doesn't always represent the reality. As machine learning and artificial intelligence get more advanced, more people are able to create so-called deep fake videos, images, and audios thanks to affordable, simple-to-use, and easily accessible video editing tools. These videos, in which real people and objects are depicted using, created, manipulated, and false film, are an increasing problem in modern culture. Pornographic deep fakes have been around for a long, but political deep fakes are a more recent issue. These frequently claimed to depict a well-known actress, model, or any other lady engaging in sex, but what is actually shown is the subject's face superimposed on the body of another woman who is engaging in the act. The simplest way to create a deep fake is by using this capability, which is referred to as face-swapping. The authors of this study applied qualitative method with analytical structural design. This paper discusses the moral, governmental, and legal ramifications of each of those deep fake classifications. The authors emphasize that, comparable to numerous other technologies in the previous, deep fakes are initially met with apprehension before becoming broadly accepted. This is because the initial uses of deep fakes were for certain evil goals (revenge porn and political campaigns). The paper additionally addresses the government's and online content distribution companies' potential roles in combating deep fakes. The report also presents a promising future scenario for how the democratization of AI can resolve the ethical issues as well as delt with current law and regulation of Bangladesh with further recommendation for deep fakes that are currently in the spotlight. The privacy and security of users will suffer as a result. Governments around the world are starting to respond to these applications that violate privacy, Bangladesh looking into TikTok's privacy concerns and enacting legislation to lessen the influence of deep fakes on society also India and other countries are banning TikTok. The deep fake's ethical and legal repercussions technology are examined in this paper, along with a number of international laws and an analysis of Bangladesh's approach to combating the deep fake crime.

Keywords: *deep-fake, AI, cyber security, privacy, moral ramifications, legal repercussions, legislations, Bangladesh, EU, India.*

[1] Author is a Legal Advisor at Bproperty.com Ltd. & Apprentice Lawyer at Dhaka Judge Court, Bangladesh.

I. INTRODUCTION

The world has seen Mr. Barack Obama, the previous president of the United States, disparage Donald Trump, a major tech figure, The assertion made by Mr. Mark Zuckerberg that "total control on billions of people's stolen data," and the profuse apologies of Jon Snow for the unexpected and uninteresting Game of Thrones finale. These are all the repercussions of deepfake. The term "deepfake" refers to a method of AI (artificial intelligence) that creates or modifies photographs of fake events using deep learning.

Synthetic media refers to automated data alteration, manipulation, and production techniques that employ artificial intelligence algorithms. The illusionary media that is accustomed to produce hoax movies, photos, and audios that are adequate persuasion to be taken for real is known as a deep fake. Deepfakes, which are frequently used with malevolent purpose, are simply any type of films, audios, or photos of any individual that have been manipulated so they look to be of someone else. These videos, in which real people and objects are depicted using, created, manipulated, and false film, are an increasing problem in modern culture. Pornographic deep fakes have become a big issue recently, despite the fact that political deep fakes are a recent problem. Face-swapping, often known as deep faking, is the process of electronically attaching face to body, one person to another. The technology employed is quite sophisticated and widely available, and there are many websites and software programs that offer a platform for face-swapping. Deep fakes pose concerns about one's reputation and privacy control on the one hand, and about one's right to free speech on the other. The privacy and security of users will suffer as a result. It is evident that the EU (European Union) and many governments around the world are aware of the problem and working to analyze and control it.

II. A TECHNOLOGICAL SUMMARY

Working with two machine learning models is a deepfake technique. One of them fabricates hoaxes using information from samples of films or photographs that are available, processing how a face can reflect various emotions, including by blinking, smirking, or smiling. When the second learning algorithm model is unable to determine whether the target's image or video that is currently available is a fake or not while the first model attempts to do so the deepfake generated product is likely to be sufficiently convincing to human eyes as well. The term "generative adversarial network" refers to this method (GAN). The cycle continues until a flawless representation of that individual is produced. It will reject erroneous samples of photos or videos, giving possibilities for new efforts to be formed. In other words, a robot powered by artificial intelligence makes a picture showing a person's expressions on their faces, while another robot continuously judges whether the image is real or phony, arguing until the final product is virtually perfect.[2]

Then, what is a Generative Adversarial Network (GAN) exactly?

A GAN consists of two adversarial neural networks (ANN), which may be used to build deep fakes. ANN can learn from unstructured audio-video material that is readily available online.[3]

The capacity to produce from a latent sample input is therefore fundamentally limited to one network, which is a generator. The distributor network is the other network that determines if the input data is genuine or not. The discriminator then assigns a score to the fake data between 0 and 1, with 1 denoting data having a high probability of being real and 0 denoting input data with a high probability of being fake. In order to prevent the discriminator from being able to the generator modifies the weights based on the discriminator's score to distinguish between the real image and the fake one it produced.

When the set of data it is designed to use is readily accessible in massive amounts, GAN performs better, which is presumably why deepfake footage frequently includes prominent names like renowned politicians, renowned actresses, and other showbiz figures. They frequently have a large number of videos available on websites, which GAN can employ to produce convincing deepfakes.

Another technique known as *Variational Auto encoders* (VAEs), which is less popular, can be used to produce deep fakes (VAEs). These, in contrast to GAN, rely on two independent networks that cooperate. This data is output by the decoder, which creates original data, while the encoder network uses it to create a dense yet smaller representation of the incoming input data. After that, the decoder can be integrated and modified to achieve the desired result. For instance, a "face swap deepfake" can be created by combining two *Variational Auto encoders*, this, in essence, superimposes a man's face on a famous person's body. In order to reproduce the original video version with a new face that is simply credible to human vision, the concerned face is encoded using that face encoder and then decoded using the famous decoder.[4]

III. Issues with deep fakes

A serious threat to civilized beings as a whole is posed by deepfakes. Deepfakes have the

[2] *What is deepfake technology?* Available at: < https://www.techslang.com/what-is-deepfake-technology/> accessed on 3 April, 2023.

[3] Hasam Khalid, Simon S. Woo, OC-FakeDect: *Classifying Deepfakes Using One-class Variational Autoencode* ,CVF, Rev. 1, 2 (2020). Available at: <https://openaccess.thecvf.com/content_CVPRW_2020/papers/w39/Khalid_OC-FakeDect_Classifying_Deepfakes_Using_One-Class_Variational_Autoencoder_CVPRW_2020_paper.pdf>

4 Raina Davis, Chris Wiggins, Joan Donovan, *Deepfakes, SPRING 2020 SERIES*, Rev, 1, (2020). Available at:<https://www.belfercenter.org/sites/default/files/files/publication/Deepfakes_2.pdf> accessed on 6 April, 2023.

potential to influence voting by propagating false propaganda via online platforms, endangering national security by generating fake news. The difficulties our technology faces are quite dangerous.

In order to classify the issues, let's first determine who produces deepfakes?[5]:

1. *Deep-fake enthusiasts* - Finding deep fake enthusiast networks is challenging. They typically enjoy swapping the faces of celebrities or regular people onto the bodies of porn stars, then producing videos in which politicians make amusing remarks, endangering marriages by releasing fake or unreal sex tapes of either spouse, or disseminating phony or false audio or video recordings of a candidate days ahead voting starts to undermine elections. One such tech-art enthusiasts often view these artificial intelligence-generated movies as a fresh type of internet fun and advocate for the advancement of this technology so that it may be used to solve riddles and not to fool or threatening others. While a few of them utilize it for their own direct personal gain, such as spreading knowledge about deepfake technology and the dangers it poses, some exploit it as art to land deepfake-related gigs for different music videos, video games, advertisements, or television shows.

2. *Political figures* - Deepfakes can be used by political figures to broadcast bogus political campaigns, disseminate phony political material, and sway public opinion. These actors include candidates, hackers, terrorists, and foreign powers. This undermines people's faith in their nation's establishments and democracy.

3. *Fraudsters* - Fraudsters currently employ artificial intelligence technology for stock manipulation and other types of financial crimes, making it a threat to society. They already imitate bank officials over the phone by employing AI-generated phony audios to request bank card information, OTPs for bank accounts, and unexpected cash transactions. Artificial super intelligence will soon be able to impersonate live video calls threaten more lives and do more harm.

4. *The Entertainment Industry*- Technologies that are deepfakes employed in a number of music videos and movie sequences after being used by game makers to give faces to the characters in their games. These are used only to support and promote the craft of filmmaking.

The following issues to the deepfake technology are further divided into: *a) Ethical issues; b) Legal issues.*

[5] Westerlund, Mika. *The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review*. 9. 39-52, (2019). Available at: <https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_ Technology_A_Review> accessed on 15 April, 2023.

(A) Ethical Issues

In recent years, this breakthrough has become more and more popular. In December 2017, a social media user going by the handle "deepfakes" demonstrated to the public how malevolent face stitching utilizing artificial intelligence methods based on neural networks is achievable. Then, via amusing and bizarre movies of well-known politicians and Hollywood personalities that were difficult to believe were fakes, deepfakes progressively acquired popularity. Recently, Deepfakes have drawn criticism from all across the world for employing technology to create fake celebrity sex recordings, false films of politicians, financial scams, as well as revenge porn.

Most of the moral issues raised by this technology fall under the categories of political both social issues.

(B) Political Issues

a. *Political disinformation* – [T]he world has seen a number of efforts at spoof films with politicians or public figures expressing their opinions and the videos becoming popular on social media platforms, all with the intention of upsetting people and spreading false information like wildfire. Deepfake technology is used to produce fake political information, which is dangerous for society. Facebook and other social media sites have been under continual pressure to delete the deep-fake content from their platforms. A phony film of Obama disparaging Donald Trump, for instance, surfaced in 2018.[6]

b. *Political and social satire* - On occasion, a false politician's face and body are used in a film with a different politician's speech that is highly lighthearted and hilarious. In that situation, the purpose of the content is to raise the social message underlying the satire rather than disseminate false facts. Facebook and other social media sites may be observed attempting to differentiate between deepfakes used for satire and deepfakes disseminating false information.

c. *Deep Fake News* - In this case, the journalism sector is hurt since it is unable to distinguish between fake and true material before disseminating it to its audience. Deepfakes are more dangerous than regular fake news since they are more difficult to spot and people tend to believe what they see as true. The technology is possible to create news videos that appear to be authentic but are actually fake and damage the news agency's image.

A news media agency can get a competitive edge today by being the first to break the news and gain access to video footage taken by a witness of an occurrence. As a result, in their haste to

[6] Raina Davis, Chris Wiggins, Joan Donovan, *Deepfakes, SPRING 2020 SERIES*, Rev, 1, (2020). Available at: <https://www.belfercenter.org/sites/default/files/files/publication/Deepfakes_2.pdf> accessed on 18 April, 2023

win the race, they frequently neglect to confirm if the video is authentic or not.[7] Videos of protests, accidents, phony protest speeches, and other events with incorrect captions that imply they occurred elsewhere and are intended to cause alarm elsewhere. For instance, Reuters in New Zealand discovered a popular video on the internet after the Christchurch mass shooting that purported to capture the moment the suspect was met by worried security personnel. Further investigation revealed that the tape was really from the USA and that the mass shooting suspect in Christchurch had not yet been slain…[8]

d. *National Security* - The days of armed conflict, military stationed in conflict areas, and the subsequent loss of life and property are long gone. Wars are being fought in this time of developing artificial intelligence both technologically and in cyberspace. In today's fake information war, putting new words in the mouth of someone in a powerful public position is a powerful weapon that foreign governments can use to influence elections, spread false political propaganda, and disrupt election campaigns in order to incite riots, violence, unrest, doubt, and distress among the electorate.

(C) Social Issues

a. *Unauthorized and retaliation-based porn* - The negative aspect of deepfakes is that this technology makes it possible to use online-available faces in pornographic content without getting their permission. Famous celebrities in this country are frequently the targets of deepfake-produced non-consensual porn. It is quite worrying because revenge porn employing deepfake can violate the victim's right to her own photos and privacy.

b. *Blackmail and extortion* - Although it is common knowledge that celebrities have fallen victim to deep-fake pornographic movies, these kinds of recordings are now also utilized against regular men, women, and children. Deeply false pornographic films using common people's faces are only uploaded with the goal to humiliate and embarrass the victim.

c. *Financial fraud and cybercrime* - [I]n these cases, the offenders frequently appeared to use deep-fake technologies to target CEOs, which can cause the victim to utter things they never intended to. A fake film of a CEO allegedly saying statements might be released by criminals, which could cause the company's stock price to drop while the culprits profit from short sells. In the foreseeable future, financial fraud and white-collar cybercrime are major concerns.[9]

[7] Westerlund, Mika. *The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review*. 9. 39-52, (2019). Available at: <https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_ Technology_A_Review> accessed on 23rd April, 2023

[8] ibid.

[9] John Bateman, *Get Ready for Deepfakes to be Used in Financial Scams, CARNEGIE FORUM FOR*

d. *Synthetic voice that sounds like a real being* - According to reports, Google is working on voice assistant capabilities that can imitate human speech and the ability to make and receive calls. Despite the fact that voice assistants like Cortana, Siri, and Alexa are regularly updated and seem more natural.[10] There are various ethical issues with artificial voices that mimic human speech. Given that it can mimic human speech, there is a significant likelihood that this synthetic voice technology will be used to extort money from people by intimidating them.

e. *Gender bias targets* - Since women make up the majority of deepfake content victims, they frequently become the targets of deepfake material that is intended to destroy their reputations or bring them disgrace. These social media sites ought to maintain that they are a secure space for everyone to have fun. Even if "involuntary synthetic pornographic imagery" was added to Google's list of prohibited content, this does not completely eliminate its production and distribution online. Deepfakes are typically made with the goal to intimidate blackmail, extort, destroy the victim's personal reputation, engage in revenge porn, and silence women. It becomes hard to delete these faked and edited films from social media sites once they are posted online (internet). Such materials frequently become popular within minutes of being shared and are repeatedly copied, downloaded, and uploaded. It becomes impossible for the relevant authorities to take down the content and find the user's IP address. This technology has opened up new channels for mistreating and demeaning women.

f. *Affecting market* - Deepfake technology is a simple tool for slandering a person, a brand, a product, a tool, or a service. This appears difficult since only a legal person may be the target of a lawsuit or legal action. Online articles that label particular items as hazardous or toxic are frequently generated utilizing the deepfake technology. Most often carried out by competing businesses to surpass market competition. The majority of the time, it is impossible to identify the author of the article or confirm who is behind the phony profile. Even if the source is found and the conduct can be justified by an alibi, it will usually be too late and the reputation may have suffered.

g. *Finding the source* - It is frequently observed that once false or changed video graphic or still footage is uploaded online, it becomes hard to take it down from the social media sites (internet). Such materials frequently become popular within minutes of being shared and are repeatedly copied, downloaded, and uploaded. It becomes more difficult for the appropriate

INTERNATIONAL PEACE, (2020). Available at: <https://carnegieendowment.org/2020/08/10/get-ready-fordeepfakes-to-be-used-in-financial-scams-pub-82469, accessed on 8 May, 2023

authorities to take down the content from online platforms and track down the IP address of the person who shared or posted it in the first place.

(D) Legal Issues

a. *Modifying the Evidence* – [D]eepfake technology has a high possibility of altering any audio-visual evidence that is to be presented in court, which would be a hurdle to discovering the truth and enforcing justice.[11] It puts a strain on our institutions' ability to redefine the parameters of truth and evidence as we provide justice in the near future.

b. *Dividend for liars* - Due to the recent tendency of media fact-checking to handle false information, a new consequence known as liar's dividend is on the rise. This phenomenon involves disproving false information, which not only extends its shelf life but also actually justifies both its existence and the discussion of its veracity. Consideration must also be given to the useful function of the liar's dividend when formulating mitigating solutions.[12] The liar's dividend, in terms of rules of proof and truth, refers to the potential of deepfakes to sow enough doubt in the public about the audio-visual material that people start claiming the authentic one as a deepfake content and fake one as the actual content.

c. *Protection of consumer* - The way some social media applications handle user data raises privacy concerns, according to the deepfake-generated social media filters. One popular Chinese app, Zao, enabled users to submit their own photos and replace their faces with characters from their favorite movies. We Chat banned the face-swapping app Zao produced material after learning that the rules of service gave users "perpetual and transferrable rights to the data posted" and caused serious privacy issues.[13]

d. *Privacy* – [T]he fear that the right to privacy may be jeopardized as a result of the publication of content containing deepfakes, which include non-consensual manipulation, embellishment, and distortion, as well as dishonest uses of non-manipulated and original video graphic content or still images for illustrative purposes.[14] The privacy debate here arises over

[11] Britt Paris, Joan Donovan, Deepfakes and Cheap Fakes: *The Manipulation of Audio and Visual Evidence, DATA SOCIETY,* (2019). Available at:<https://datasociety.net/wp-content/uploads/2019/09/DataSociety_Deepfakes_Cheap_ Fakes.pdf > accessed on 10 May, 2023

[12] Paul Chadwickl. The Liar's Dividend, and Other Challenges of Deep-Fake News, *THE GUARDIAN. GUARDIAN NEWS AND MEDIA* (2018). Available at:<https://www.theguardian.com/commentisfree/2018/jul/22/deep-fake-news-donald-trump-vladimir-putin,> accessed on 12 May, 2023

[13] 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, 2020). Available at:<https://www.cnbc.com/2019/09/04/chinese-faceswapping-app-zao-takes-dangers-of-deepfake-to-the-masses.html> accessed on 14 May, 2023

[14] David Fink, Sarah Diamond, *Deepfakes: 2020 and Beyond*, LAW.COM, (2020). Available at:<https://store.law.com/Registration/Login.aspx?mode=silent&source=https%3A%2F%2Fwww.law.com%2Ft her ecorder%2F2020%2F09%2F03%2Fdeepfakes-2020-and-beyond%2F> accessed on 18 May, 2023

the use of celebrity faces as well as faces of regular people in non-consensual pornography content. It is frequently asserted that when altered, publicly shared audiovisual information turns private.[15]

e. *Delayed Content Identification* - The notion of the liar's dividend states that the detection of deep fakes always occurs after their creation. Simply said, this indicates that there is likelihood that the majority of people will have ingested the deepfake information by the time it is found and deleted. Policymakers must think about how to take proactive steps to reduce any potential harm that may result from the dissemination of a deepfake created.

f. *Political and individual freedom* - Deepfakes' involvement in manufacturing and disseminating false information and fake news puts the fundamental idea of free and fair elections in jeopardy. Deepfakes are capable of making fake news and social media material faster than any human writer. By doing so, the right to political participation and the right to personal freedom are threatened. Similar to how individuals may simply use AI-powered deepfake technology to promote the dissemination of false information or are able to influence political public discourse, they can easily use it to generate, disseminate, and distribute false material intended to instigate war or any other type of violence that might endanger both human life and property with their wicked and evil objectives.[16]

g. *Defamation* - A deepfake material may contain anything, including video graphic content that has been edited or created from scratch or still images. An individual with public importance saying things in a video that he is not supposed to say, for example, or a video of someone sharing private information about someone else that often turns out to be true. The content creator may have published the video for entertainment purposes or for any other reason. The person whose private information is exposed in the first instance is the victim of defamation, but the person in the second instance is the victim of defamation since his image has been harmed and derogated by the manner he is shown in the film. It is a technology that, if improperly governed, might hurt people from all socioeconomic classes.

h. *Targeting women* - Since women make up the majority of deepfake content victims and frequently fall for posting non-consensual sexual material or any other type of deepfake material with the intention of damaging her reputation or humiliating her. These social media sites ought to maintain that they are a secure space for everyone to have fun. Even if "involuntary synthetic

[15] Clare McGlynn, Erika Rackley & Ruth Houghton, Beyond 'Revenge Porn': *The Continuum of Image-Based Sexual Abuse*, Fem Leg Stud 25. Rev.25, 46 (2017).Available at:<https://doi.org/10.1007/s10691-017-9343-2> accessed on 20 May, 2023

[16] *Human rights in the age of Artificial Intelligence.* Available at:<https://www.accessnow.org/cms/assets/uploads/2018/11 /AI-and-Human-Rights.pdf. Cal. Elec. Code § 20010(a) (2020)> accessed on 25 May, 2023

pornographic imagery" was added to Google's list of prohibited content, this does not completely eliminate its production and distribution online. Deepfakes are typically made with the goal to intimidate blackmail, extort, destroy the victim's personal reputation, engage in revenge porn, and silence women. The problem for policymakers is to safeguard women's safety through tougher regulations, in addition to data protection and privacy.

IV. Bangladesh's position in dealing with crime related to deepfake

Recent events involving deepfake revenge porn and the use of deepfake technology in political campaigns as well as on social media platforms like Facebook, YouTube, and Tiktok have also occurred in Bangladesh.

Combining technology and law is now the doable response to the impending harm posed by this technology. The growing trend of fabricating political campaigns and pornographic movies using this deep-fake technology raises various problems about issues with privacy and identity theft, as well as the realism and validity of elections and the material on social media platforms.

Deep fakes are not specifically addressed by any laws. Numerous causes of action that currently exist in our current laws may be expanded to include deepfake offences. The following provisions are only a few of them:

1) Defamation:

In Bangladesh, a person is subject to civil and criminal liability for the act of defamation. Another possibility is to file a defamation complaint in order to pursue legal action against deepfake crime.

Yet, in Bangladesh, defamation is frequently used incorrectly.

Section 499 of The Penal Code 1860 says-Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or published any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation or such person, is said, except in the cases hereinafter excepted, to defame that person.[17]

Whoever defames another person shall be punished with simple imprisonment for a time which may extend to two years, or with fine, or with both, according to section 500 of the Criminal Code 1860.

Nonetheless, the majority of defamation lawsuits in Bangladesh are solely filed for harassment.

[17] Penal Code,1860

Defamation cases are dismissed at relatively modest costs in lower courts as a result. Yet, under Section 198 of The Criminal Process of 1898, anybody who feels defamed may file a lawsuit. To stop crimes relating to defamation from being misused, there is another statute. The Digital Security Act of 2018 is that. But, this law is unable to halt the abuse of the defamation offense. So, we must strengthen the laws that deal with defamation.[18]

2) *Data protection law*

The terrible reality is that there are no regulations governing data protection or privacy. The right to privacy is guaranteed under our Constitution's Article 33(b). He/she may file a case in the High Court Division under Article 102(1) if this right is infringed.

Everyone has the right to have their data protected securely, according to section 7 of the Right to Information Act of 2009. Nobody is going to publish their data. No one or any authority has the right to access his data. The Digital Security Act of 2018's provisions can be used to stop the abuse of personal data. These options, however, fall short.

3) *Control of Pornography Legislation*

Pornographic or "revenge porn" videos make up the majority of Deepfake's productions. The majority of the victims in this case are female. The 2012 Pornography Control Act can be used as assistance. The Pornography Regulation Act of 2012, section 8, severely restricts pornography and imposes a wide variety of penalties. According to section 8 (1), any act that records video or still images of sexual conduct or behavior that exposes sexual feeling, with or without the knowledge of the individuals involved in the sexual contact, is punished by a maximum sentence of 8 years in jail and a fine of 2 lac taka. Making pornographic videos involving minors is a severe felony that carries a 10 year prison sentence and a 5 lac taka fine, according to Section 8(6).

4) *Tort Law*

Tort law is connected to the use of a person's name, resemblance, or personality for commercial gain. Yet regrettably, the utilization of tort law is quite scarce in Bangladesh. Tort law is relevant to the crime committed by deepfake. The victim may be entitled to compensation under tort law. Hence, in order to obtain compensation for deepfake crime, tort law should be applied.

5) *Copyright Infringement*

Deepfake materials may contain a modified form of the audio or visual effects from either a music video or movie, which could constitute a copyrighted work. According to the Copy Right

[18] ibid.

Act of 2000, the owner of a cinematographed music video or movie has the sole authority to obtain a license for the purpose of creating another duplicate of the film, as well as any image or sound it contains.

In the case of *Amarnath Sehgal vs. Union of India*[19] , Delhi High Court, the author's moral right was acknowledged. The author is entitled to compensation for any act of mutilation, distortion, or change that would be detrimental to his reputation and infringe upon his moral authority over his work. In the event that the moral rights to the licensed work are violated, the Copyright owner may be entitled to compensation, injunctions, and other legal remedies as provided by law.[20]

Yet, since movie producers—not actors—typically run the danger of being the target; these remedies may not be beneficial for the victim of a deepfake content. The same is true for images and photos; the photographer owns the copyright, not the person being photographed. So, it's possible that the remedies provided by this legislation won't help the actual victim or target of the deepfake material.

V. Recommendations

1. Laws and legislations - stringent rules and regulations are one strategy for combating deepfakes. To deal with the crimes associated to deepfakes within its legal purview, the state laws now in place against defamation, identity fraud, data theft, privacy, copyright, etc. can be strengthened. Strong penalties and large fines for producing profound false material may serve as a brake on the rate of technological advancement and the danger it poses to society. The authorities also set regulations that draw a narrow line between deep-fake content produced for self-expression under the freedom of expression and content that breaches one's right to privacy.

2. protection of consumers' privacy - The developers and suppliers of social media services can create and employ methods to warn consumers when they are seeing deep-fake content on their site. There should be a cap on how far the terms and conditions of the service providers' privacy policies may go before they end up abusing the information and privacy of their customers. The development of secure digital infrastructure should be prioritized.

3. Education and awareness - To counteract deepfake materials, awareness and education are essential. The general public should be informed of these AI-generated technologies' potential dangers and be able to avoid falling for their deep-fake contents. Moreover, teaching young people about the dangers of promoting or spreading fake information online Also, the

[19] Copy Right Act, 2000

[20] 117 (2005) DLT 717.

general public has to be educated on how to spot material that is profoundly false and offered on internet media platforms.

Some of the minor cues that can be used to spot information that has been edited or created artificially include[21]

a) The deep-fake content's generated face's eyes may not blink naturally or may do so in an odd way. The blinks wouldn't follow the pattern of a typical human blink.

b) It is frequently observed that the created face's lip synching is either off or not in rhythm with the music. The audio visual mismatch in that situation is fairly obvious.

c) An unnatural lip sync may also cause the movement of the teeth to appear odd.

d) Facial muscles move in an abnormal way, and thus the skin's texture is uneven.

e) If someone had long hair, the way the hair moved would appear out of the ordinary.

4. Social media platforms' accountability

The well-known social media sites like Facebook, Twitter, TikTok, Instagram, Snapchat, and others that allow its users to submit and share material must have some ethical and social obligation to forbid or restrict the publication of deepfake information. As women make up the majority of deepfake content victims, they frequently become the targets of deepfake content that harms their reputations or publishes non-consensual pornography. These social media sites ought to maintain that they are a secure space for everyone to have fun.

5. Marking the fabricated content

People frequently assume that the deep-fake information they see online is authentic, but the reality often proves to be quite different. One method is to utilize video fingerprinting to add disclaimer watermarks to the content, such as "false content" or any other acceptable watermark, when it is initially posted on any internet site. This, to a certain extent, can aid in finding a solution to the issue.

VI. Conclusion

Every day, new technology is developed. There are new developments in the field of technology every day. Law does not, however, advance at such a rapid rate, and the current legal systems in Bangladesh and numerous other nations do not have any legislation that primarily controls deepfakes. The deepfake challenges may not be adequately addressed by current regulations

[21] David Fink and Sarah Diamond, *Deepfakes: 2020 and Beyond*, LAW.COM (2020). Available at:<(https://www.law.com/therecorder/2020/09/03/deepfakes-2020-and-beyond/)> accessed on 8 June, 2023

without the use of technical techniques.

In terms of cyber security, these topics have been hotly contested for years. Yet it is also our moral duty as a community to work to stop the spread of harmful information that is not in line with the majority opinion. Educating ourselves about manipulations and the damage they may do, and raising awareness of them. Kids should be educated on the repercussions of fabricating information online and posting, downloading, or distributing it. To ensure that the source of the information is recognized and appropriately restricted, authorities should be on the lookout for novel approaches to controlling deepfakes. A common defense used against fraudulent content is that a person has the right to free speech and expression guaranteed under Article 39 of the Constitution of the People's Republic of Bangladesh, 1972.

It must be remembered that one's right to privacy begins where our freedom of expression stops. Here, it is our responsibility to recognize that neither our freedom nor our actions tend to impede anybody else from using their rights. The proper platforms, including but not limited to government agencies, social media, and business goliaths, should deploy artificial intelligence algorithms to detect and stop deepfakes.

*****