Journal of Strategic Security

Volume 17 | Number 3 Article 5

Regulating Deepfakes: An Indian perspective

Shinu Vig
Symbiosis Centre for Management Studies, Noida, India, shinu.vig@scmsnoida.ac.in

pp. 70-93

Recommended Citation
Vig, Shinu. "Regulating Deepfakes: An Indian perspective." *Journal of Strategic Security* 17, no. 3 (2024) : 70-93.
DOI: https://doi.org/10.5038/1944-0472.17.3.2245
Available at: https://digitalcommons.usf.edu/jss/vol17/iss3/5

Regulating Deepfakes: An Indian perspective

Abstract

Deepfakes are a growing concern throughout the world including India. Deepfakes can be used for several purposes, both innocuous or malicious. In India, several problems related to regulation of deepfakes have emerged. This paper makes an examination of current legal challenges posed by deepfakes as well as solutions in India that can be repurposed to address these challenges, including intellectual property laws, criminal laws, and the right to privacy. While these existing laws can be used to address certain aspects of the deep fake problem, there is an increasing recognition that specific legislations and regulations addressing deep fakes and synthetic media are urgently needed. Moreover, substantial efforts are required to be made to raise awareness, develop countermeasures, and establish a legal framework to mitigate the risks associated with this technology.

Introduction

Deepfakes are a growing concern throughout the world including India. Deepfakes are manipulated or synthetic media, often created using artificial intelligence techniques like deep learning, to convincingly alter or generate videos, audio recordings, or images. They can be used for various purposes, both benign and malicious. Deepfake technology is based on an advanced algorithm which produces hyper-realistic videos using a person's face, voice or likeness by utilizing machine learning techniques. These fake videos or audios are then manipulated to appear as if the person is saying or doing certain things.[1] Deepfakes, characterized by their strikingly realistic appearance, are generated through the utilization of artificial intelligence applications that merge various technologies to produce a new audio or video clip. This process involves the overlaying, modification, and fusion of images, ultimately culminating in the creation of a complex and convincing video.[2] Deepfakes adopt the form of face reenactment, face generation, face swapping, and speech synthesis. Deepfakes in the form of face reenactment means a software manipulates the facial features of an individual, while face generation means a novel countenance is formed that does not possess any association with a particular individual. Furthermore, they are also evident in face swapping, whereby the face of one person is exchanged with that of another, and in speech synthesis, where voices are reconstructed.

Deepfake technology, despite its potential for misuse and ethical concerns, also has some potential benefits and applications. The utilization and progression of deepfake technology as a medium for enhancing various industries, including healthcare and entertainment, holds vast potential.[3] Notably, in the healthcare sector, deepfake has demonstrated significant diagnostic advantages, as evidenced by studies conducted by several scholars.[4] In the entertainment industry it can be used for dubbing and language localization. Additionally, in the tourism industry, the photorealistic imageries created by the use of technology are particularly valuable for marketing and advertising purposes.[5] These pictures might elicit positive emotions towards a destination.[6] It also provides businesses opportunities for user co-innovation.[7] Moreover, high-resolution media pictures have the ability to make a favorable impression, whereby tourists can participate in co-creating the destination image through social media platforms.[8] In education, deepfake technology can create realistic simulations for training purposes, such as medical training simulations or military exercises. It can help in language learning by providing learners with conversations featuring native speakers. Deepfake information distinctly diminishes the expenditure of content production.[9] The transformation of text paragraphs into various styles of images via deepfake technology presents a more cost-effective and enhanced resolution for illustrations in literature. Subsequently, deepfake information can resolve the issue of inadequate data in numerous fields.[10] For instance, the effectiveness of self-driving automobiles relies on deepfake data to perform road tests in a simulated environment, enabling the testing of billions of miles at a reduced cost.[11]

The present manuscript will concentrate on the deleterious consequences attributed to the utilization of deepfakes, which have been identified as the most pressing artificial intelligence-related criminal hazard.[12] The emergence of deepfakes has instigated considerable distress within the community as they can be implemented to manipulate the public's mindset by fabricating various types of media, including counterfeit pornographic or political clips of an individual without their endorsement, consequently compromising their personal and professional life. At first glance, the credibility of deepfakes might appear substantiated to its viewers; however, its prevalence has resulted in the dissemination of fallacious information in a pervasive manner.[13] The increasing plausibility of such media is becoming increasingly disconcerting as technology improves, leading to effortless distribution and a wider audience. Several technology experts have cautioned that deepfakes will soon become so sophisticated that they will be undetectable. Therefore, it has become a matter of utmost urgency to critically scrutinize the means of controlling the proliferation of illicit and pernicious deepfakes and the role that digital platforms can undertake in addressing this threat. Regulatory and ethical guidelines are required to address these challenges and ensure that deepfake technology is used in ways that benefit society while minimizing harm.

Previous research has predominantly concentrated on technical identification of deepfake information.[14] While others have focused on aspects concerning its detection.[15] However, there have been a few studies pertaining to the ethical implications of deepfake information including issues such as violations of privacy, cyberbullying, defamation, identity theft, and harassment.[16] In this background, the primary aim of the current paper is to augment the existing pool of knowledge by presenting a concise outline and analysis of the challenges and relevant laws pertaining to the use of deep fakes in India. There is a scarcity of studies that explore the issues surrounding deep fakes, particularly in context of India. Consequently, the paper endeavors to address three primary research questions. First, what challenges arise as a result of the emergence of deep fakes? Second, what are the applicable provisions in Indian laws and regulations? Third, what measures might be implemented to reinforce these laws to effectively tackle the challenges posed by deep fakes?

Methodology

This study employed a qualitative research methodology, wherein primarily secondary data was used. The secondary sources included the relevant Indian laws and regulations. Consultation with professionals and legal experts involved in the field of technology was also a source of information. A doctrinal research method was followed for the paper.[17] It draws heavily upon the existing works such as published research studies and legal texts, including acts, policies, reports, and websites of regulatory bodies relating to technology.[18] To achieve the objectives of the paper, a desk research approach was utilized to identify relevant legal texts, published materials, and scientific works.

Challenges Posed by the Use of Deepfakes

The emergence of deepfake information presents a multitude of hazards and complexities and has raised concerns across various domains. [19] The swift development of deepfake technology has brought to light an escalating apprehension regarding their applications. These concerns primarily stem from the creation of an environment lacking in trust, as well as the possible exploitation of vulnerable and unsuspecting individuals by unscrupulous hackers and scammers. This section discusses the challenges posed by the use of deepfakes.

Misinformation and Fake News

Deepfakes are being applied to create convincing fake content, including videos, audio content, and images, which can be used to spread false or misleading information. Inaccurate depictions, which can be indistinguishable from genuine content, can be manipulated to defame, deceive, and engage in other forms of misconduct.[20] Deepfakes can be used to compromise reputations, subvert democratic processes, and undermine trust in legitimate online sources of authenticated data. Within the Global Risks Report 2024 by the World Economic Forum misinformation and disinformation are identified as the foremost peril confronting the global community in the next two years.[21] The ramifications of deepfakes on public confidence hold substantial importance. When applied to distort the image of politicians, public servants, and business leaders, they have the capacity to diminish individuals' trust in governmental bodies, media platforms, legal frameworks, and private establishments.

In contrast to conventional disinformation, deepfake information is imbued with heightened realism, persuasiveness, plausibility, and dissemination intent.[22] As a result, viewers may develop erroneous beliefs due to the prevalence of deepfake news.[23] Deepfake videos have the potential to distort collective recollections of public events.[24] This can have serious consequences for public perception, trust, and decision-making. Deepfakes, possess the potential to be utilized in a malicious manner for the purpose of spreading misinformation or defaming individuals. As a result, the identification and detection of Deepfakes play a critical role in enhancing the credibility of social media platforms and other media-sharing websites.[25] The easy accessibility of audio-visual content through social media, coupled with the accessibility to modern tools such as Tensorflow or Keras, AI software, and cost-effective computing resources, along with the swift advancement of deep-learning (DL) methods, specifically Generative Adversarial Networks (GAN), has facilitated the creation of deepfakes with the intention of disseminating disinformation, monetary frauds, hoaxes, and disrupting government operations.[26] Deepfake content can spread rapidly on social media and other online platforms, making it challenging for victims to control the dissemination of false information or to clear their name.

India’s unfortunate reputation as the disseminator of misinformation is linked to its high rate of Internet usage and the growing trend of social media engagement. The country boasts a staggering 323 million internet users, with 67% residing in urban areas and the remaining 33% in rural regions. The lack of media literacy stands out as a pivotal element contributing to the proliferation of misinformation during the pandemic.[27] Throughout the COVID-19 pandemic, false information regarding remedies and therapies spread rapidly through various social media channels in India. One notable case revolved around a widely circulated video promoting the consumption of cow urine as a preventive or curative measure against COVID-19. Despite being discredited by health authorities, the video amassed millions of views and played a role in the dissemination of misinformation, thereby posing potential health hazards as certain individuals embraced and acted upon the inaccurate content.

Political Manipulation

Political deepfake information may have an influence on the attitudes of recipients toward politicians.[28] Deepfake news with high source vividness amplifies the credibility and engagement intention of fraudulent news.[29] There have been numerous occurrences worldwide where deepfakes have been employed to advance political interests by exploiting the likeness and image of renowned political figures. These individuals may be portrayed as using a racial epithet, accepting a bribe, and admitting to complicity in a crime, among other things.[30] In the United States, a manipulated video of Nanci Pelosi, the Speaker of the House, went viral in 2019, wherein she was depicted as if she were slurring her speech.[31] In the United Kingdom, the think tank Future Advocacy released deepfake videos of Boris Johnson and Jeremy Corbyn, which portrayed them as endorsing each other for the position of Prime Minister. According to Future Advocacy 2019 it was done to increase awareness of the dangers surrounding political disinformation and the methods used by parties during elections to mislead the public. The potential danger presented by deepfakes in the political landscape is significant. This is evidenced by the use of manipulated videos during election campaigns for the purpose of advancing particular political objectives or besmirching the character of an opposing leader. The use of deepfakes for malicious purposes may lead to political instability. The potential impact of deepfakes on fair elections and democracy as a whole is a matter of great concern.[32] In 2020, India witnessed its first-ever use of AI-generated deepfake technology in political campaigning when several deepfake videos of politician Manoj Tiwari were circulated on WhatsApp groups. These videos depicted Tiwari making accusations towards his political rival Arvind Kejriwal in both English and Haryanvi languages, preceding the elections in Delhi, the Indian capital state.

In a diverse and politically sensitive country like India, deepfakes can exacerbate existing communal tensions, incite violence, and erode trust in democratic institutions, leading to social unrest and instability.

Foreign state and non-state actors may have an interest in destabilizing India, particularly during elections, by exploiting deepfake technology. Countries with strained diplomatic relations or territorial disputes with India may seek to undermine its stability and influence public opinion through the dissemination of deepfake content. This could include neighboring countries like Pakistan or China, which have geopolitical interests in the region. Non-state actors such as terrorist organizations operating in the region may seek to exploit deepfake technology to spread propaganda, incite violence, undermine the democratic process in India, or to breach the national security of the country. By exploiting vulnerabilities in the information ecosystem, these actors can amplify existing social and political divisions, erode trust in democratic institutions, and destabilize the electoral process in India.

The issue of political deepfakes also has the potential to significantly impact the field of journalism as well as the overall quality of democracy. These manipulated videos can lead viewers to question the authenticity of the content, resulting in decreased levels of trust in social media news.[33] Additionally, politicians may use real videos as a defense against accusations by claiming they are deepfakes, a tactic known as the ‘liar's dividend’.[34] If left unaddressed, political deepfakes could prove to be perilous not only for those directly involved but also for the general public who may find themselves unsure of which news sources to believe, leading to a lack of trust in online information. Therefore, safeguarding against the malicious use of deepfake technology is essential for protecting the integrity of Indian elections and preserving democratic norms and principles.

Cyberbullying and Harassment

Individuals can be targeted through deepfake technology, with malicious actors creating fake content to harass or defame them online. Deepfakes can be used to manipulate and cheat people by making it appear as if someone is saying or doing something that they never did. This might include creating fake videos of persons engaged in illegal or immoral activities, making false statements, or engaging in inappropriate conduct. The majority of deepfakes encountered on the internet are of a pornographic nature.[35] The inception of deepfake pornography began to spread several years ago when a Reddit user shared doctored videos of actresses with their faces swapped onto the bodies of porn actors.[36] Since then, numerous unauthorized videos have been uploaded to various websites by deepfake creators, with many famous individuals such as actors, journalists, and public figures being targeted, resulting in harm to their image and brand. In fact, certain websites are commercially misusing this technology by offering users the ability to create their own deepfakes and facilitating the creation of unauthorized sexual videos of other people without their consent or knowledge.

As highlighted by several studies, this technology could also be exploited to commit crimes such as revenge pornography, blackmail, and extortion. Women are the exclusive victims of deepfake pornography, which can harm their dignity. Being targeted by deepfake-based cyberbullying can have severe social and psychological consequences for the victim. They may experience shame, embarrassment, and damage to their reputation. In some cases, it can lead to emotional distress and even mental health issues. For example, in the year 2023, two Indian actresses- Rashmika Mandanna and Priyanka Chopra Jonas, fell prey to deepfake as their images and voice were manipulated using deepfake technology.

Privacy-Related Concerns

Deepfakes can be used to create explicit or damaging content using the faces of individuals without their consent, leading to privacy violations and potential harm to personal and professional reputations. Creating deepfakes often requires access to personal photos or videos of the target individual. This can involve a significant invasion of privacy, as the cyberbully may use private or intimate content without consent. The safeguarding of data privacy has captured significant attention in recent times. Concerns related to online privacy can be broadly classified into seven dimensions: control, awareness, collection, secondary use, errors, improper access, and post-remedies.[37] The protection of privacy is deemed an ethical obligation, prompted by concerns surrounding the secondary use of personal information. Individuals are wary of the unsanctioned use of their personal data by deepfake information service providers and users.[38] The risk of privacy breach acts as a crucial precursor to public opposition against deepfake information. This article will center its attention on the plausible concerns regarding privacy, predominantly encompassing defamation, false light as well as the entitlement of publicity, which is also occasionally recognized as personality rights.[39] The term 'Right of Publicity' commonly pertains to the concept of 'Personality rights'. This legal right grants an individual the authority to regulate the commercial exploitation of their name, image, likeness, or identity. It is typically classified as a property right rather than a personal one. Statutes in numerous countries acknowledge the Right of Publicity. However, if a video is created by superimposing the face of a person by using deep fake technology, this implies a violation of these rights.

Frauds Through Impersonation

Frauds through impersonation using deepfakes represent a serious and growing concern in the realm of cybersecurity and digital identity theft. Impersonation deepfakes involve the use of artificial intelligence and machine learning techniques to create convincing simulations of someone's appearance, voice, and behavior, often with the intention of deceiving others for fraudulent purposes. If deployed in commercial settings, deepfakes and bots have the potential to result in catastrophic outcomes. The impersonation attack is of paramount significance, if not more so, as it has emerged as one of the most critical issues in view of the adoption of face as the primary authentication mechanism in numerous applications.[40]

Impersonation deepfakes can be used to defraud individuals, businesses, or organizations. For example, scammers may create deepfake videos or voice recordings of executives or employees to request unauthorized wire transfers, divulge sensitive information, or engage in fraudulent activities. Individuals with malicious intent could utilize deepfake voice phishing techniques to impersonate renowned business leaders, thereby deceiving customers into fraudulent activities and causing financial losses. In December 2023, the co-founder and CEO of Zerodha Broking Ltd., a leading Indian stockbroker and financial services company, expressed apprehensions regarding the escalating risk posed by generative artificial intelligence (AI) technology and deepfakes to the financial service sector. Within a video disseminated on X (formerly known as Twitter), he highlighted the challenges encountered in authenticating customer identities due to the prevalent digitalization. The Zerodha co-founder disseminated a 58-second video on X and Instagram. The visual content appeared unremarkable until Nikhil himself revealed towards the conclusion that the video was created using his deepfake avatar.

Deepfakes can be used for identity theft by impersonating individuals in various contexts, such as social media, video conferences, or phone calls. Attackers can use this impersonation to gain access to personal accounts, and sensitive data, or even commit crimes in the victim's name. Deepfakes can be incorporated into phishing campaigns and social engineering attacks. Cybercriminals may use deepfake emails, messages, or phone calls to trick individuals into revealing personal information, login credentials, or financial details. Deepfake impersonation can harm the reputation of individuals and organizations. False statements or actions attributed to someone through deepfakes can have long-lasting and damaging consequences.

Another big threat is in the financial domain, whereby gullible citizens are coaxed or threatened through deep fakes into transferring money into the criminal's account. In such an instance, in April 2024, a businessman from Mumbai, India, was swindled out of Rupees 80,000 in an AI voice cloning scam. The victim received a call allegedly from the Indian embassy in Dubai, wherein he was informed that his son was arrested and sentenced to imprisonment. He was asked to transfer money for the payment of the bail amount. The businessman believed it as his son's voice was cloned and hence, transferred the amount to the fraudsters.

Legal Framework in India

These challenges posed by deepfakes discussed in the previous section highlight the need to regulate the usage of deepfakes through legal mechanisms. In India, till now, there is no legislation that specifically addresses the issue of deepfakes. India can develop a comprehensive and effective approach to tackling the challenges posed by deepfakes by taking inspiration from other countries like the USA. US federal and state lawmakers have been taking various measures to address the problem of deepfakes, primarily focusing on legislation and policy initiatives. The Malicious Deep Fake Prohibition Act was introduced in the U.S. Senate in 2019. This bill sought to criminalize the creation and distribution of deepfake content with the intent to deceive the public, particularly during elections. The Identifying Outputs of Generative Adversarial Networks (IOGAN) Act, introduced in 2020, proposed establishing a task force within the Department of Homeland Security to study deepfake technology and develop strategies to counter its harmful effects. DEEPFAKES Accountability Act was introduced in the U.S. House of Representatives in 2023. This bill aimed to protect national security against the threats posed by deepfake technology and to provide legal recourse to victims of harmful deepfakes. In the absence of specific laws for addressing deepfakes in India, there are existing Indian laws that can be repurposed to apply to the same. These have been discussed hereafter.

Right to Privacy

International human rights law offers a distinct and global structure to encourage and safeguard the 'right to privacy'. Article 12 of the Universal Declaration of Human Rights (1948) duly acknowledges the 'right to privacy' as an inherent human right. In accordance with this provision, it is impermissible and unlawful to arbitrarily infringe upon an individual's honor or reputation. Moreover, the right to privacy has been solemnly acknowledged as a fundamental right to life by virtue of Article 21 of the Constitution of India, as affirmed in the KS Puttaswamy v. Union of India (2017) legal decision. According to this judgment, an individual's right to privacy encompasses their ability to exercise control over the dissemination of personal information, which is both necessary and imperative. This also encompasses the unconsented and unauthorized utilization of deepfakes in any conceivable manner, as it has the potential to undermine one's standing and unduly encroach upon their personal autonomy.

Furthermore, the Digital Personal Data Protection Bill of 2022 explicitly addresses the safeguarding of personal data pertaining to natural persons, that may be collected online or offline and subsequently digitized. The utilization of such data is limited solely to lawful and consensual usage. In the event of a data breach, individuals possess the right to request the rectification and removal of information obtained by a data fiduciary, who may face severe penalties. Additionally, the proposal includes the establishment of a Data Protection Board, enabling consumers to file complaints should the data fiduciary fail to provide a satisfactory resolution. As the Bill awaits passage as an Act in India, its actual impact remains to be observed. Nevertheless, its scope could potentially encompass the unauthorized dissemination and utilization of deepfakes.

However, there has been a conflict between the government and social media companies as far as the right to privacy is concerned. The conflict between the Indian government and social media companies primarily revolves around the implementation of the new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules, introduced by the Indian government in February 2021, aim to regulate social media platforms, digital news publishers, and OTT (Over-The-Top) platforms operating in India. These rules compel encrypted social media messaging platforms to disclose their users' identities if demanded by the government. The new IT rules introduced provisions holding social media intermediaries accountable for user-generated content on their platforms. Companies failing to comply with the rules risk losing intermediary status, thereby becoming liable for any illegal content posted by users. Social media companies have expressed concerns about being held responsible for user-generated content beyond their control, while the Indian government maintains that intermediaries must take proactive measures to prevent the spread of harmful content and ensure accountability for their platforms' use.

This conflict between the government and social media companies regarding the right to privacy reflects broader tensions between security interests, regulatory oversight, freedom of expression, and individual privacy rights in the digital age. Finding a balance between these competing interests requires ongoing dialogue, collaboration, and transparency between governments, social media companies, civil society, and other stakeholders to uphold privacy principles while addressing legitimate concerns related to security, law enforcement, and public safety.

Right of Publicity

The concept commonly known as the 'Right of Publicity' can also be referred to as 'Personality rights'. This concept grants individuals the authority to regulate the commercial utilization of their name, image, likeness, or identity. It is widely acknowledged as a form of property right rather than a personal right. Statutes in numerous countries recognize the existence of the Right of Publicity. John Locke argued that the economic value associated with one's identity should be attributed to the celebrity individual, as it is primarily a product of their labor. In the context of deepfakes, Locke's theory of identity remains relevant in several ways. Locke's emphasis on consciousness and memory raises questions about the authenticity of experiences depicted in deepfake videos. Deepfakes can be used to manipulate individuals' identities by superimposing their faces onto the bodies of others or altering their speech in videos. If a deepfake convincingly portrays someone saying or doing something they never actually did, it blurs the line between reality and fabrication, potentially affecting how their identity is perceived. This manipulation can have serious implications for individuals' reputations, relationships, and even safety. Locke's theory highlights the importance of consciousness and memory in shaping one's identity and suggests that the manipulation of these aspects through deepfakes can undermine individuals' sense of self and autonomy.

The ‘right of publicity’ serves to safeguard the interests of celebrities regarding the use of their images and identities. An interesting illustration of its application can be observed in the recent history of the ‘right of publicity’. This refers to the entitlement of celebrities to prohibit or seek compensation for commercial portrayals or imitations of their facial features, vocal characteristics, distinctive expressions, trademark poses, and similar aspects.[41]

There exists no explicit legislative provision with respect to the extent and application of the right of publicity in the jurisdiction of India. Indeed, the right of publicity is acknowledged in India, albeit not as an independent lawful right. Although no precise legislation pertaining to the right of publicity is in existence, the law courts of India have acknowledged the right of publicity as a legally enforceable right by the medium of judicial decisions. The right to publicity is an inherent facet of the right to privacy, which is provided under Articles 19 and 21 of the Indian Constitution. Delhi High Court has opined that the entitlement to the right of publicity is exclusive to a person or any manifestations of his/her persona, such as their name, personal attributes, autograph, or vocal characteristics (ICC Development (International) Ltd v Arvee Enterprises, 2003). Consequently, solely an individual concerned is eligible to derive pecuniary benefits from the right of publicity. Additionally, the right of publicity is transferable, thus it may be transferred to the legal heirs of the person subsequent to their demise. It should be noted, however, that presently there is an absence of any specific statutory provision or legal precedent in India that explicitly upholds this inheritance concept. In the same case, the Delhi High Court had provided a comprehensive interpretation of the term ‘publicity rights’ and noted that the term encompasses an individual's persona, including their signature or voice. In the absence of a specific statutory provision, the violation of the right of publicity is not explicitly demarcated under any Indian law. Nevertheless, the unauthorized utilization of a celebrity's persona, image, or information amounts to a violation of their right to publicity and might be legally contested as such. Thus, if a deepfake uses the image or voice of a well-known person, then it amounts to a violation of their right to privacy.

Criminal Laws

Moreover, Indian law encompasses regulations that criminalize fraudulent activities, which encompass acts such as identity theft and financial fraud. The perpetration of identity theft and virtual forgery through the utilization of deepfakes can constitute severe consequences and yield far-reaching ramifications for both individuals and society at large. The deployment of deepfakes with the intention of pilfering an individual's identity, fabricating fictitious portrayals of people, or manipulating public sentiment can inflict harm upon an individual's reputation, as well as propagate disinformation. The invocation of Sections 420 and 468 of the Indian Penal Code, 1860 could potentially be warranted in this context. These sections provide for punishment in the form of imprisonment and fine, in case of cheating and forgery.

Information Technology Laws

Section 66E of the IT Act of 2000 is applicable in cases pertaining to deepfake offenses encompassing the capturing, dissemination, or transmission of an individual's visual representations through mass media, thereby infringing upon their right to privacy. This transgression carries the potential penalty of imprisonment for a duration of three years or a monetary fine amounting to ₹2 lakh. Another pertinent provision within the IT Act is Section 66D. It encompasses the legal framework to prosecute individuals who employ communication devices or computer resources with malicious intentions, aiming to deceive or assume the identity of another person, thereby exposing them to the prospect of incarceration for a period of three years and/or a monetary fine up to ₹1 lakh. These particular sections of the IT Act can be invoked to hold accountable those individuals implicated in deepfake cybercrimes within the jurisdiction of India.

The utilization of deepfakes for the dissemination of false information, the subversion of the Government, or the incitement of hatred and disaffection towards the Government is a matter of utmost concern and possesses the potential to yield extensive consequences for society. The propagation of inaccurate or deceiving data has the capability to instigate confusion and undermine the trust of the general public. Additionally, it can be employed as a means to manipulate public sentiment and exert influence over political outcomes. These crimes can be subject to legal prosecution under Section 66-F (cyber terrorism) of the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022. The propagation of hate speech and online defamation through the utilization of deepfakes can engender consequential predicaments that have the potential to inflict harm upon both individuals and society on a collective level. The utilization of deepfakes as a vehicle for the dissemination of hate speech or defamatory content has the capacity to inflict substantial damage upon the repute and overall welfare of people, thereby contributing to the cultivation of a harmful online atmosphere. In accordance with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 of the Information Technology Act, 2000, the perpetration of these crimes can be subject to legal prosecution.

The accountability of intermediaries might also be questioned, as these intermediaries serve as the platforms where the deepfake content is uploaded and consequently are subjected to the regulations outlined in Section 79 of the Information Technology Act, 2000. As per this provision, the intermediary is permitted to remove the content in question once they become aware of its existence or upon receiving a judicial order. But in the case of Myspace Inc. v Super Cassettes Industries Ltd (2017), the Court ruled that in situations involving infringement of copyrights, the intermediaries are obligated to remove the infringing material upon receipt of a notice from private parties, even if a Court order is not explicitly issued.

As stipulated by the Information Technology Rules of 2021, Social Media Intermediaries (Intermediaries with registered users exceeding a specified threshold) must designate specific individuals tasked with monitoring and ascertaining the source of information as well as certain forms of content. Moreover, these rules additionally offer guidelines to intermediaries to establish a mechanism for the resolution of grievances, thereby addressing the concerns, complaints, and dissatisfactions voiced by users. In November 2023, the Indian government issued a Directive to the ‘social media intermediaries’ to remove morphed videos or deepfakes from their platforms within 24 hours of a complaint being filed, in accordance with a requirement outlined in the IT Rules 2021. The instructions came after the deepfake videos of two actors surfaced online within the span of one week.

Copyright Laws

The Indian Copyrights Act, 1957 and Copyright Rules, 1958 encompass the legal framework for the safeguarding of copyrights. The Copyright Act underwent significant amendments in 2012. Given that India adheres to a common-law system, it is grounded in judicial precedents. Moreover, India is a signatory to the Berne Convention and Universal Copyright Convention. It enacted the International Copyright Order in 1999, which deals with the copyright protection of foreign works. As per the Copyright Act, 1957, "the term 'work' includes an artistic work comprising of a painting, a sculpture, a drawing (including a diagram, a map, a chart or plan), an engraving, a photograph, a work of architecture or artistic craftsmanship, dramatic work, literary work (including computer programs, tables, compilations, and computer databases), musical work (including music as well as graphical notations), sound recording and cinematographic film." Indian legislation offers copyright protection for various forms of artistic expression, such as films, music, and other forms of creative content.

If an individual utilizes copyrighted material without permission to create deepfakes, copyright holders have the right to initiate legal proceedings against the infringing party. The Indian Copyright Act of 1957, specifically Section 51, establishes penalties for specific offenses related to copyright infringement. This provision explicitly prohibits the unauthorized utilization of another individual's property, particularly if said property is subject to exclusive ownership. Deepfakes, which encompass the unsanctioned manipulation or modification of extant photos and videos, may be deemed to encroach upon the copyright proprietor's entitlement to reproduction of the copyrighted material in the event that a significant segment is replicated. By virtue of deepfakes being creations founded upon pre-existing works, these can also be regarded as derivative works. As copyright law confers the exclusive right to produce derivative works solely upon the copyright owner, the act of creating and disseminating deepfakes without authorization would be deemed as copyright infringement.

Possible Solutions

Reducing the problem of deepfakes is a complex and ongoing challenge. It requires a multi-pronged approach involving government, industry, and civil society. The section below discusses several actions the government can take to help mitigate the threat of deepfakes.

Legal Approach

At present there is no law in India that directly deals with deepfakes. The term ‘deepfakes’ has not been defined under any Indian law either. Deepfake technology refers to the use of artificial intelligence (AI), machine learning algorithms, and advanced image and audio processing techniques to create highly realistic synthetic media content that falsely portrays individuals or events. Wherein synthetic media refers to media generated or manipulated with the usage of artificial intelligence. Providing a clear definition of deepfake technology in Indian law shall enable policymakers, law enforcement agencies, and judicial authorities to identify and distinguish deepfake-related offenses from other forms of digital manipulation or misinformation. A clear definition shall lay the foundation for developing targeted legal frameworks and regulatory measures to address the challenges posed by deepfake technology effectively.

Though the term ‘deepfakes’ has not been defined under Indian law there are several other laws, as discussed above that may be applicable to deepfakes. In this scenario, it is important to delve into the existing legal framework to identify the loopholes. The laws that provide legal remedies against deepfakes require a legal action to be filed in a court of law. However, these legal claims inadequately address the potential impact of deepfakes on public opinion, the harm caused to the reputation of the individual portrayed, and the violation of privacy and dignity when utilized in contexts such as pornography. The identification of the uploader can be a challenging task, and the time gap between initiating legal proceedings and obtaining a court order may prove to be insufficient if the deepfake becomes widely spread. Deepfakes are characterized by their remarkable speed and amplification capabilities. Hence, they have opened the door to malicious applications of this relatively new technology.[42] In the context of the digital age, it is incumbent upon social media platforms to fulfill their social duty by actively monitoring and removing deepfake content.

The AI regulatory framework will be the most pertinent regulatory framework for law enforcement in the realm of deepfakes. EU has made substantial progress in the realm of AI regulation. EU has reached initial agreement for the implementation of the world’s first ‘Artificial

Intelligence Act' which aims to classify and regulate AI-based systems on the basis of the level of their risk implications (EUIPO, 2024).[43] While the AI Act generally does not discourage the use of AI, it forbids the use of AI in multiple application scenarios or makes its use dependent on various technical, organizational, and legal requirements. The Act further makes the producers of general-purpose AI systems accountable for furnishing the material used to train their models and to comply with the EU copyright laws.

India has, however, adopted a distinct approach to AI regulation wherein it prioritizes harnessing its potential rather than strict regulation. The law in India provides for intermediary responsibility and proactive monitoring by the intermediaries. However, the extent of intermediary liability in India remains uncertain. The dual approach of the Copyright and the Information Technology Act has left numerous inquiries unresolved.[44] The obligations of intermediaries have increased due to their improved technological proficiency. The Information Technology Act, together with its associated guidelines, indicates the continually expanding capability of intermediaries and imposes a mandatory compliance framework on them. In an effort to keep pace with emerging innovations, the legislation in India is progressively moving towards stringent regulation of the more recent and advanced functions that intermediaries undertake. A potential measure that could prove beneficial is the establishment of distinct and clear guidelines by the government for specifically addressing deepfakes.

India could consider implementing laws that focus on prevention, early intervention, and swift response to potential deepfake-related offenses to act as a deterrent to perpetrators before a crime is committed. Introducing laws that require internet platforms and social media companies to implement proactive measures to detect and remove deepfake content before it spreads can be effective. Mandating the use of content moderation algorithms, digital watermarking, and other automated tools to identify and flag potentially harmful deepfakes can help prevent their dissemination and mitigate their impact.[45] The Indian government can also make laws requiring internet service providers, social media platforms, and other online intermediaries to monitor and report suspicious deepfake activity to law enforcement agencies in real time. This can facilitate early detection and intervention and enable authorities to take prompt action to prevent the spread of harmful deepfakes.

Indian policymakers can also strengthen its legal framework to combat the proliferation of deepfakes and protect its citizens from potential harm by enacting laws that impose severe penalties, including fines and imprisonment, for individuals or entities found guilty of creating, distributing, or using deepfakes for malicious purposes can deter potential perpetrators. Establishing clear legal consequences for engaging in deepfake-related offenses sends a strong message that such actions will not be tolerated and will be met with swift and decisive punishment.

Technological Approach

While the creation of laws and regulations is necessary there is also a need for technology that may aid in moderation of content hosted on the internet and social media platforms. Thus, one of the most obvious approaches to managing Deepfakes involves the utilization of technological remedies. Technological remedies adopt a proactive approach to detecting Deepfakes, identifying them in advance of their potential wide dissemination across major social media platforms, such as Instagram, Facebook, or YouTube. The government can allocate resources for research and development to detect and combat deepfakes. It might support academic institutions, research labs, technology companies, and startups in developing tools and technologies to identify and verify content authenticity. The government bodies might also work closely with technology companies to establish industry standards for content authentication and deepfake detection which might encourage the development and deployment of deepfake detection tools on popular social media platforms.

In order to address the challenges posed by deepfake technology, it is imperative to understand what kind of action other actors, including the online platform companies where most deepfakes are shared, are addressing this threat. In this context, Meta (formerly Facebook) announced a new policy banning deepfakes from their platforms in 2020. Meta said it would take down AI-edited content that would likely mislead the public, but clarified that satire or parodies using the same technology would still be permissible on the platforms. Hence, law enforcement agencies are required to be aware of the policies technology companies have put in place, as it is likely that potential evidence or malicious content will be shared via these platforms. How technology companies such as Twitter and Meta regulate deepfake technology will have an extensive impact on how people will engage with and react to deepfakes. Apart from making organizational policies, various technology companies are working on deepfake detection technologies. Meta informed the development of an AI tool that detects deepfakes by reverse engineering a single AI-generated image to track its origin. Google released a large dataset of visual deepfakes that has been incorporated into the FaceForensics benchmark. Microsoft launched the Microsoft Video Authenticator, which can analyze a still photo or video to provide a percentage chance of whether the media has been artificially manipulated.[46] The current regulations only focus on online takedowns in the form of censorship or criminal prosecution but lack a deeper understanding of how generative AI technology works and the wide range of harm that it can cause. Establishing partnerships with tech industry stakeholders to share expertise, data, and best practices can facilitate the development of innovative solutions to address the challenges posed by deepfakes.

Several international organizations have also taken initiatives to tackle this problem. The World Economic Forum’s Digital Trust Initiative, initiated in 2022, aims to counter these negative consequences by ensuring technology is developed and used in a way that protects and upholds society’s expectations and values. The Forum’s Global Coalition for Digital Safety also advocates for a whole-of-society approach that mobilizes governments, the private sector, and citizen groups to build media and information literacy to combat disinformation. The European Union (EU) has allocated funding for research projects aimed at developing technologies to detect and mitigate the impact of deepfakes. For example, the EU's Horizon 2020 program has supported various research projects focused on cybersecurity, including efforts to combat disinformation and fake news, which are often facilitated by deepfake technology.

While the EU's approach to engaging with the tech industry has shown promise, it may not be directly replicable in the Indian context due to several challenges, such as differences in technological infrastructure, regulatory and legal framework and cultural and sociopolitical factors. While India could draw insights from the EU's approach to countering deepfakes, it would be necessary to tailor strategies to suit the country's specific context and address the challenges inherent in its socio-cultural, technological, and regulatory landscape. Collaboration between the government, tech industry, academia, and civil society would be critical to developing and implementing effective solutions to combat the spread of deepfakes in India.

Digital Literacy Approach

The existing IT Rules only address the instances wherein the deepfake content has already been uploaded and the resultant harm has been suffered; instead, the regulatory bodies are required to put more emphasis on preventive measures, for instance, making users aware that they are looking at a morphed image. The challenge to regulate deepfakes is coupled with a public that seems relatively ignorant about the dangers of deepfakes and, hence, might be unable to identify deepfakes (videos, photos, audios) since they are not aware of the existence of such virtual forgeries or how are they done. The lack of understanding of the basics of this technology presents numerous challenges for law enforcement agencies. This challenge can be curtailed through informative initiatives and digital literacy programs.

Digital literacy encompasses the act of enlightening individuals about the existence of Deepfakes on social media platforms and their potential to impact individuals' choices and viewpoints. The efficacy of media literacy as a remedy for the consequences of Deepfakes has been well-recognized. The government might launch public awareness campaigns to educate people about the existence and risks of deepfakes. It might teach people how to identify potential deepfake content and verify information. Digital literacy programs can also be integrated into school curricula, and training programs can be offered for adults to enhance media literacy and critical thinking skills. This can empower individuals to recognize and resist the spread of deepfake content. In a country like India, which has a large population, Government bodies might also seek support from media literacy organizations by providing financial support to such organizations that focus on media literacy and fact-checking initiatives. These organizations can play a crucial role in debunking deepfake content.

Implications

This study has implications for regulators and policymakers as the increasing utilization of deepfake technology has given rise to apprehensions regarding the necessity of more robust legal frameworks in order to tackle concerns related to privacy, data protection, and cybercrime. Although India does possess certain legislations that can be employed to combat deepfake technology, additional legislation that specifically addresses the distinctive challenges posed by deepfakes is required. One challenge that arises is the absence of a precise legal definition of deepfake technology and the actions that are considered as deepfake-related offenses. This lack of clarity can create difficulties in prosecuting individuals or organizations that engage in malevolent or deceitful activities utilizing deepfakes.

The current legislation pertaining to cyber offenses caused by deepfakes in India is insufficient in its entirety to adequately address this problem. The absence of specific provisions within the IT Act of 2000 concerning artificial intelligence, machine learning, and deepfakes renders the effective regulation of these technologies quite challenging. In order to more effectively regulate offenses resulting from the utilization of deepfakes, it may be imperative to revise the IT Act of 2000 to encompass legal provisions that explicitly target the usage of deepfakes and the corresponding penalties for their misapplication. This may involve imposing heightened penalties for those who engage in the creation or dissemination of deepfakes for malicious motives, as well as establishing more robust legal safeguards for persons whose images or likenesses are utilized without their permission. In the meanwhile, it is imperative for both people and organizations to possess knowledge regarding the possible hazards correlated with deepfakes and to exercise vigilance when verifying the genuineness of material available on the internet.

The study also has several significant social implications. It emphasizes the role of media literacy programs to empower individuals in identifying and resisting the spread of misinformation through deepfake content. The government can foster partnerships with civil society and media literacy organizations to run public awareness campaigns. These initiatives shall sensitize the public about the existence and risk of deepfakes and protect them from its negative consequences. Till the time the regulatory revisions are implemented, it is imperative for both people and organizations to possess knowledge regarding the possible hazards correlated with deepfakes and to exercise vigilance when verifying the genuineness of material available on the internet.

Conclusion

The increasing utilization of deepfake technology has generated apprehensions regarding the necessity for more robust legal structures to tackle concerns such as privacy, data security, and cybercrime. Although India possesses certain legislations that can potentially be employed to counteract deepfake technology, there is an exigent requirement for more precise statutory measures to effectively confront the distinctive hurdles presented by deepfakes. There is a growing awareness in India on the usage of deepfakes. In addition to the aforementioned legal provisions, the Ministry of Information and Broadcasting, on January 9, 2023, issued a cautionary directive to media entities, urging them to exercise prudence when disseminating content that may be subject to manipulation or tampering. Furthermore, the Ministry advised media organizations to explicitly label any manipulated content as ‘manipulated’ or ‘modified’ to ensure that viewers are cognizant of the fact that the content has been altered. Although India currently lacks specific legislation that directly pertains to the matter of deepfakes, there exist legal provisions and government initiatives that hold the potential to address this concern. As the prevalence and sophistication of deepfakes continue to increase, it is probable that the Indian government will take additional measures to tackle this issue and safeguard individuals from potential harm. It is also crucial to acknowledge that the creation and utilization of deepfakes represent a global concern, necessitating international cooperation and collaboration to effectively regulate their usage and avert infringements upon privacy.

Endnotes

[1] Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, “The State of Deepfakes: Landscape, Threats and Impact,” Deeptrace, accessed July 21, 2023, https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

[2] Molly Mullen, “A New Reality: Deepfake Technology and the World Around Us,” Mitchell Hamline Law Review 48 (2022): 210.

[3] Geraint Rees, “Here's How Deepfake Technology Can Actually Be a Good Thing,” in World Economic Forum Agenda, 2019.

[4] Mika Westerlund, “The Emergence of Deepfake Technology: A Review,” Technology Innovation Management Review 9, no. 11 (2019).

[5] Patricia Picazo and Sergio Moreno-Gil, “Analysis of the Projected Image of Tourism Destinations on Photographs: A Literature Review to Prepare for the Future,” Journal of Vacation Marketing 25, no. 1 (2019): 3-24.

[6] Sixing Chen, Jun Kang, Suchi Liu, and Yifan Sun, “Cognitive Computing on Unstructured Data for Customer Co-innovation,” European Journal of Marketing 54, no. 3 (2019): 570-593.

[7] Sameer Hosany, Daniela Buzova, and Silvia Sanz-Blas, “The Influence of Place Attachment, Ad-evoked Positive Affect, and Motivation on Intention to Visit: Imagination Proclivity as a Moderator,” Journal of Travel Research 59, no. 3 (2020): 477-495.

[8] Marija Cimbaljević, Uglješa Stankov, and Vanja Pavluković, “Going Beyond the Traditional Destination Competitiveness–Reflections on a Smart Destination in the Current Research,” Current Issues in Tourism 22, no. 20 (2019): 2472-2477.

[9] Anupama Chadha, Vaibhav Kumar, Sonu Kashyap, and Mayank Gupta, “Deepfake: An Overview,” in Proceedings of Second International Conference on Computing, Communications, and Cyber-Security: IC4S 2020 (Singapore: Springer, 2021), 557-

DOI: https://doi.org/10.5038/1944-0472.17.3.2245

566.

[10] Mika Westerlund, "The Emergence of Deepfake Technology: A Review," Technology Innovation Management Review 9, no. 11 (2019).

[11] Minghui Li and Yan Wan, "Norms or Fun? The Influence of Ethical Concerns and Perceived Enjoyment on the Regulation of Deepfake Information," Internet Research (2023).

[12] Matthew Caldwell, Jerone TA Andrews, Thomas Tanay, and Lewis D. Griffin, "AI-enabled Future Crime," Crime Science 9, no. 1 (2020): 1-13.

[13] Abdul-Rahman, Kabbara. "Bots & Deepfakes." NSI Intern Integration Project, August 2021. https://nsiteam.com/social/wp-content/uploads/2021/08/IIJO_eIntern-IP_Bots-and-Deepfakes_Kabbara_FINAL.pdf.

[14] Aya Ismail, Marwa Elpeltagy, Mervat Zaki, and Kamal A. ElDahshan, "Deepfake Video Detection: YOLO-Face Convolution Recurrent Approach," PeerJ Computer Science 7 (2021): e730.

[15] Sawinder Kaur, Parteek Kumar, and Ponnurangam Kumaraguru, "Deepfakes: Temporal Sequential Analysis to Detect Face-swapped Video Clips Using Convolutional Long Short-term Memory," Journal of Electronic Imaging 29, no. 3 (2020): 033013.

[16] Carl Öhman, "Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography," Ethics and Information Technology 22, no. 2 (2020): 133-140.

[17] Shinu Vig, "Intellectual Property Rights and the Metaverse: An Indian Perspective," The Journal of World Intellectual Property 25, no. 3 (2022): 753-766.

[18] Mauritz Kop, "AI & Intellectual Property: Towards an Articulated Public Domain," Texas Intellectual Property Law Journal 28 (2019): 297.

[19] Keith Raymond Harris, "Video on Demand: What Deepfakes Do and How They Harm," Synthese 199, no. 5-6 (2021): 13373-13391.

[20] Vasileia Karasavva and Aalia Noorbhai, "The Real Threat of Deepfake Pornography: A Review of Canadian Policy," Cyberpsychology, Behavior, and Social Networking 24, no. 3 (2021): 203-209.

[21] World Economic Forum, "Global Risk Report 2024," accessed May 14, 2024, https://www.weforum.org/publications/global-risks-report-2024/.

[22] Yoori Hwang, Ji Youn Ryu, and Se-Hoon Jeong, "Effects of Disinformation Using Deepfake: The Protective Effect of Media Literacy Education," Cyberpsychology, Behavior, and Social Networking 24, no. 3 (2021): 188-193.

[23] Chandell Gosse and Jacquelyn Burkell, "Politics and Porn: How News Media Characterizes Problems Presented by Deepfakes," Critical Studies in Media Communication 37, no. 5 (2020): 497-511.

[24] Gillian Murphy and Emma Flynn, "Deepfake False Memories," Memory 30, no. 4 (2022): 480-492.

[25] Paarth Neekhara, Brian Dolhansky, Joanna Bitton, and Cristian Canton Ferrer, "Adversarial Threats to Deepfake Detection: A Practical Perspective," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2021): 923-932.

[26] Momina Masood, Marriam Nawaz, Ali Javed, Tahira Nazir, Awais Mehmood, and Rabbia Mahum, "Classification of Deepfake Videos Using Pre-trained Convolutional Neural Networks," in 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2) (IEEE, 2021), 1-6.

[27] Ashish Sharma, "India's Floating Disinformation During the COVID-19 Pandemic," Journal of Media Ethics 37, no. 2 (2022): 145-147.

[28] Tom Dobber, Nadia Metoui, Damian Trilling, Natali Helberger, and Claes de Vreese, "Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?" The International Journal of Press/Politics 26, no. 1 (2021): 69-91.

[29] Jiyoung Lee and Soo Yun Shin, "Something That They Never Said: Multimodal Disinformation and Source Vividness in Understanding the Power of AI-enabled Deepfake News," Media Psychology 25, no. 4 (2022): 531-546.

[30] Abdul-Rahman Kabbara. "Bots & Deepfakes." NSI Intern Integration Project, August 2021. https://nsiteam.com/social/wp-content/uploads/2021/08/IIJO_eIntern-IP_Bots-and-Deepfakes_Kabbara_FINAL.pdf.

[31] CBS, "Doctored Nancy Pelosi Video Highlights Threat of 'Deepfake' Tech," CBS News, May 26, 2019, https://www.cbsnews.com/news/doctored-nancy-pelosi-video-highlights-threat-of-deepfake-tech-2019-05-25/.

[32] Lindsey Wilkerson, "Still Waters Run Deep (Fakes): The Rising Concerns of 'Deepfake' Technology and Its Influence on Democracy and the First Amendment," Missouri Law Review 86 (2021): 407.

[33] Cristian Vaccari and Andrew Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," Social Media + Society 6, no. 1 (2020): 2056305120903408.

[34] Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics," Foreign Affairs 98 (2019): 147.

[35] Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, "The State of Deepfakes: Landscape, Threats and Impact," Deeptrace, accessed July 21, 2023, https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

[36] Sophie Maddocks, "A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities Between Pornographic and 'Political' Deep Fakes," Porn Studies 7, no. 4 (2020): 415-423.

[37] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke, "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," MIS Quarterly (1996): 167-196.

[38] Weiyin Hong and James YL Thong, "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," MIS Quarterly (2013): 275-298.

[39] Erik Gerstner, "Face/Off: 'DeepFake' Face Swaps and Privacy Laws," Defense Counsel Journal 87 (2020): 1.

[40] Shahroz Tariq, Sowon Jeon, and Simon S. Woo, "Am I a Real or Fake Celebrity? Evaluating Face Recognition and Verification APIs Under Deepfake Impersonation Attack," in Proceedings of the ACM Web Conference 2022 (2022): 512-523.

[41] Kevin M. Fisher, "Which Path to Follow: A Comparative Perspective on the Right of Publicity," Connecticut Journal of International Law 16 (2000): 95.

[42] Emma Perot and Frederick Mostert, "Fake It Till You Make It: An Examination of the US and English Approaches to Persona Protection as Applied to Deepfakes on Social Media," Journal of Intellectual Property Law & Practice 15, no. 1 (2020): 32-39.

[43] EUIPO, "Navigating the Complexities of Generative AI in Intellectual Property: Challenges and Opportunities," 2024, https://www.euipo.europa.eu/en/news/navigating-the-complexities-of-generative-ai-in-intellectual-property-challenges-and-opportunities.

[44] Indranath Gupta and Lakshmi Srinivasan, "Evolving Scope of Intermediary Liability in India," International Review of Law, Computers & Technology (2023): 1-31.

[45] Ling-Yuan Hsu, "AI-assisted Deepfake Detection Using Adaptive Blind Image Watermarking," Journal of Visual Communication and Image Representation (2024): 104094.

[46] EUROPOL, "Facing Reality? Law Enforcement and the Challenge of Deepfakes," accessed May 17, 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf.

DOI: https://doi.org/10.5038/1944-0472.17.3.2245