IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Deepfake Crimes And Legal Regulation In India: A Comprehensive Analysis.

Krishang and Aastha

ABSTRACT-

Deepfake technology is a modern and sophisticated technology that has eventually eradicated the fine line between being real and fake. It is an evil approach with the use of artificial intelligence (AI) to make the unreal look real. Deepfake has its impact which has taken the turn of cybercrime across the country and the world as a whole. The victimisation of individuals to the trap of deepfake approaches has hiked which needs to be taken into serious concern. Here, we are going to discuss about deepfake crimes in India and the need for a necessary legal structure in the country to regulate deepfake crimes. We will also look into certain approaches by other countries to combat the same.

INTRODUCTION-

The revolutionary progress in artificial intelligence and machine learning has, regrettably, spawned a deeply disturbing phenomenon - the rise of Deepfakes.

Deepfakes are digitally manipulated media, primarily videos, that employ these advanced technologies to fabricate realistic-looking content, often by superimposing one person's likeness onto another's body. The technology behind this extraordinary phenomenon is known as Generative Adversarial Networks, a machine learning framework that pits two neural networks against each other - one generates synthetic data, while the other tries to distinguish it from real data. The malicious applications of deepfakes are manifold and concerning, as they can be used to create false narratives, discredit public figures, perpetrate financial fraud, and even produce non-consensual explicit content.

India, as a rapidly emerging global power and a technological hub, has not been spared from the scourge of deepfake crimes. The legal landscape in India, however, remains in flux, as existing laws struggle to keep pace with the evolving threats posed by this technology. The need for some new legal policies can be felt as the technology around us is rapidly advancing. Especially regarding the Indian scenario, it is of paramount importance that the law is aligned with the rise of these new threats brought about by this rapid technological advancement, to protect the masses who are unaware or lack the adequate knowledge to protect themselves from these newfound cyber offences.

This comprehensive analysis delves into the multifaceted nature of deepfake crimes in India, examining the various forms they take and the profound impact they have on individuals, institutions, and society as a whole. It then scrutinizes the current legal framework in India, assessing its adequacy in addressing the

unique challenges presented by deepfakes and identifying the pressing need for legislative reforms to enhance the protection of citizens' rights and the preservation of truth in the digital age.

UNDERSTANDING DEEPFAKE TECHNOLOGY-

Artificial intelligence technology is a far more advanced innovation of mankind than ever before. Among the many breakthroughs in this field, the emergence of deepfake technology, which leverages Generative Adversarial Networks, has garnered significant attention due to its profound impact on various facets of our digital landscape. A Generative Adversarial Network is a deep learning framework that comprises two neural networks, a generator and a discriminator which are put against each other in a game-like scenario, where the generator aims to produce synthetic data that is indistinguishable from real data, while the discriminator strives to differentiate between the two accurately. The generator network is trained to progressively enhance the realism and authenticity of its outputs, continuously refining its capabilities to the point where its creations become increasingly hard to discern from genuine data, while the discriminator network is meticulously trained to scrutinize these synthetic contents, honing its skills to detect even the most subtle discrepancies in the produced output. The more time the process takes, the more sophisticated the generated content becomes, blurring the line between reality and fiction. This dynamic interplay between the generator and the discriminator lies at the heart of Deepfake technology, enabling the creation of highly convincing, yet entirely fabricated, multimedia content that includes images, audio, and video.

The potential applications of Deepfake technology are wide-ranging, spanning from entertainment and artistic expression to more sinister use cases in the realm of cybercrime. Now as we speak about the negative aspect of deepfake technology, it poses a significant threat to individuals, organizations, and even societies as a whole, as it empowers malicious actors to create highly convincing fake content for nefarious purposes. The technology can be used for misinformation campaigns, financial fraud, identity theft, and reputational damage. Deepfakes can also be deployed to manipulate public opinion by disseminating false information or propaganda. This has created a significant challenge to trust and credibility in the digital age.

EMERGING TREND OF DEEPFAKE CRIMES IN INDIA-

The emergence of crimes in the society has always created disruption and disturbance amongst citizens and crimes related to deep fakes have simply added to it. Deepfakes have a remarkable contribution in creating more crimes in the society.

Multiple innocents as well as intellectuals have been fooled and became victims to deepfake scams. The concordant increase in the crime rates has brought about significant disaster to many lives and there are numerous testaments to it.

Sources say, since 2019, there has been a remarkable escalation of deepfake cases by 550% calling for losses to about Rs. 70,000 crores in 2024 alone. Again, according to 2024 reports by Pi-Labs there has been a prominent surge of epidemic of deepfake frauds. It is also estimated that, Deepfakes mask 40% of the AI generated cyber crimes and over one million deepfake videos have been reported in 2024 around the globe.

There are innumerable cases of deepfake crimes in India that have acquired the spotlight in the recent past. In 2022, Kerala faced its first deepfake reported case. Radhakrishnan, a 73-year-old man became victim to such a fraud through a phone call and consequently it led to him losing Rs. 40,000. Similarly, a case happened in Madurai, to a banker who received a phone call from a stranger claiming his son to be in danger and

demanding a sum of Rs. 5000. There are multiple such cases that have grappled with society. It has eradicated the line between real and fake. It has also made people confused and lose trust in authenticity and security.

There is a significant increase in the development of AI technology which has eased work life by its sophisticated nature. Regardless of these advancements, proper organisational awareness is limited and people are left vulnerable. The available mechanisms and strategies to those cyber criminals to cause fraudulent escalate the crime rates and hence, the efforts to alleviate such crimes go in vain.

FINANCIAL IMPLICATIONS, CYBERBULLYING AND THE PSYCHOLOGICAL IMPACTS ON INDIVIDUALS-

The proliferation of deepfakes has introduced a new dimension to online harassment, blurring the lines between reality and fabrication, with potential financial and psychological consequences for targeted individuals. The people targeted with deepfakes usually comply with the cybercriminals due to the realistic nature of the content created to manipulate and coerce individuals, potentially leading to financial losses. Deepfakes can be exploited for malicious purposes such as identity theft, fraud, and extortion, thereby causing substantial financial harm to the victim and their associates. The sophisticated manipulation of audio and video content in deepfakes undermine the credibility of digital media, eroding public trust in online information sources and making it increasingly challenging for individuals to discern authentic content from fabricated content.

Excluding the immediate financial risks, the psychological impact of deepfakes on targeted individuals can be extensive, potentially triggering a spectrum of adverse emotional and cognitive responses and impacting their overall well-being. Furthermore, the potential for deepfakes to damage personal and professional reputations can have far-reaching consequences for victims, affecting their relationships, career prospects, and social standing within their communities.

The use of deepfakes in cyberbullying campaigns represents a disturbing evolution of online harassment tactics, amplifying the potential for emotional distress and psychological harm. Victims of deepfake related cyberbullying may experience a range of negative emotions, including shame, anger, anxiety, and depression, as they grapple with the violation of their privacy and the dissemination of false or defamatory content. The persistent nature of online harassment, compounded by the viral spread of deepfakes, can create a hostile and inescapable environment for victims, exacerbating feelings of isolation and helplessness and decreasing their self-esteem. The anonymity afforded by the internet can embolden perpetrators to engage in more egregious forms of harassment, shielded from accountability and amplifying the psychological toll on victims. In addition to the immediate emotional impact, deepfake-related cyberbullying can have long-lasting consequences for victims' mental health, potentially leading to chronic anxiety, post-traumatic stress disorder, and suicidal ideation.

Thus, we can see the impact that deepfakes have on individuals extends far beyond mere reputational damage, encompassing significant financial risks, psychological trauma, and profound disruptions to personal and professional lives. Deepfakes present unprecedented challenges for individuals navigating the digital landscape, requiring proactive measures to mitigate the risks and protect against potential harm.

EXISTING LEGAL FRAMEWORK IN INDIA AND ITS LIMITATIONS-

There is an abiding legal regulation for every crime in different countries with respect to their laws and a strict framework for the legal regulations is essentially important for the crimes and those in association with deepfake cases as well.

India doesn't currently have any prominent law or regulation to cope with deepfake crimes. The Information Technology Act, 2000 (IT Act) has certain provisions under a few sections that deal with such crimes. Section 66(D) and Section 66(E) of the Information Technology Act, 2000 penalise a person for impersonating another individual or uploading any private space in electronic form across social media. And again, Section 67, 67(A) and 67(B) of the IT Act, 2000 punish an individual engrossed in any activity of publishing and transiting sexually offensive content.

The Indian legal regulations and provisions are not yet enough to carry out procedures to deal with deepfake cases and hence, inspiration can be acquired from other countries in terms of provisions and frameworks to tackle such issues in the country. India can introduce certain provisions like The Malicious Deepfake Prohibition Act, 2019 or The Identifying Outputs Of Generative Adversarial Network (IOGAN) Act, 2020 that are introduced in the U.S. DEEPFAKE Accountability Act was introduced in the U.S. House of Representatives in 2023 which aimed at fostering national security against threats posed by Deepfake frauds. India has a long way to go in terms of framing a legal structure promoting provisions and regulations to suppress crimes rates posed by Deepfakes.

The basic human rights - *Right to Privacy* or *Right to Publicity* are some of the most innate fundamental rights. Article 12 of the Universal Declaration of Human Rights (1948) recognises *Right to Privacy* as one of the intrinsic human rights. According to the Indian Constitution, Article 21 represents *Right to Life* and privacy is a basic right that a human is born with and they cannot be deprived of it. As it is evident in the landmark case of K.S. Puttaswamy (Rtrd.) & Anr. V. Union of India & org. which is also known as the *Right to Privacy Verdict,* where the Supreme Court held that the *Right to Privacy* is protected as a fundamental right under the Articles 14, 19 and 21 of the Indian Constitution. The original petitioner was Justice K.S. Puttaswamy, a former judge of the Karnataka High Court.

Right to Publicity is an individual's legal right to profit or control the utilisation of their name, image or likeness, protecting them from unauthorised exploitation. Although the right is not specifically codified under any law, it is derived from the *Right to Privacy,* enshrined under its umbrella, benefitting public figures who have a commercial value in association with their personality.

Hence, we have understood that the regulatory framework in the legal background stabilises the crime rates and brings a considerate reduction to the intensity of its occurrence. India has a long way to go or maybe it has not yet begun. The existing framework doesn't suffice and therefore a rigid structure would foster a clearer and more organised regulation of the deepfake crimes in India.

COMPARATIVE LEGAL ANALYSIS: GLOBAL APPROACH

The exponential growth of artificial intelligence and deepfake technologies poses intricate challenges to legal systems globally, demanding a meticulous evaluation of current legal structures and the formulation of innovative regulatory strategies. This analysis undertakes a comparative examination of the legal frameworks in India, the United States, the United Kingdom, and China, scrutinizing their approaches to AI and deepfake regulation, while highlighting the nuances, strengths, and limitations inherent in each jurisdiction. Navigating this complex terrain necessitates a comprehensive understanding of technological advancements, ethical

considerations, and the imperative to balance innovation with the protection of individual rights and societal values.

In the Indian context, the legal landscape concerning AI and deepfakes remain largely nascent, characterized by the absence of specific legislation tailored to address the unique challenges posed by these technologies. While existing laws, such as the Information Technology Act, 2000, offer some recourse against cybercrimes and online fraud, their applicability to AI-related harms and deepfake dissemination is limited and often requires interpretive stretching. The absence of a dedicated legal framework creates ambiguity and uncertainty, hindering effective enforcement and leaving individuals vulnerable to potential misuse of AI and deepfake technologies.

The United States, while not having a single, comprehensive AI law, addresses AI and deepfakes through a patchwork of existing laws and regulations, including those related to defamation, fraud, and intellectual property. Federal agencies, such as the Federal Trade Commission, have taken enforcement actions against deceptive AI practices, but the lack of specific AI legislation has led to calls for a more comprehensive and coordinated approach.

Similarly, the United Kingdom relies on existing laws, such as the Defamation Act 2013 and the Computer Misuse Act 1990, to address harms caused by AI and deepfakes. The UK government has also issued guidance on AI ethics and governance, but these are non-binding and do not have the force of law.

China, in contrast, has taken a more proactive approach, enacting specific regulations to govern AI and deepfake technologies. These regulations, while demonstrating a commitment to AI governance, have also raised concerns about potential restrictions on freedom of expression and innovation.

A comparative analysis reveals a spectrum of regulatory approaches, ranging from the reactive, patchwork approach of the US and UK to the more proactive, but potentially restrictive, approach of China, with India lagging behind in terms of specific legal frameworks. This disparity underscores the need for international cooperation and the development of best practices to ensure responsible AI development and deployment while safeguarding fundamental rights and promoting innovation.

To conclude, the legal and regulatory landscape surrounding AI and deepfakes is rapidly evolving, with jurisdictions grappling with the challenge of balancing innovation, ethical considerations, and the protection of individual rights.

CONCLUSION -

The bond between humans and developing technology has got firmer with time. The inclination of mankind towards technological dependency has enhanced and in every walk of life, Artificial Intelligence technology has acquired a stake.

With evolving technology, we have witnessed prominent drawbacks that follow the advancement of human life entangled with technology. As we have discussed enough and known about the drawbacks or setbacks accompanying developing trends, we see the extent of harm technology can bring to an individual through various windows. One of them, which is yet to acquire a remarkable spotlight is the deepfake crimes. The country and its people have faced multiple deepfake cases being recklessly victimised. In recent times, we have also looked-on the emerging trend of fraud which counts for fraud calls which also lie under deepfake crimes.

The Indian structure for regulating such crimes needs its way to the system to control and bring a halt to such crimes. Delving into technological pleasure has controlled human activities and hence, many times, people failed to understand the consequences of certain technological misuse. With changing trends and developing technology, a developed system and structural background for regulation of crimes related to technology is the call of the time and such an emergence is awaited in India.