DEEPFAKE AND PERSONALITY RIGHTS: AN EMERGING CYBER-IPR CONFLICT

by

Rohan Gupta

1. INTRODUCTION

New artificial intelligence technologies have great potential to promote and protect human rights. Its predictive skills have the potential to revolutionize criminal justice systems by reducing the number of wrongful convictions and increasing the number of fair trials, while also improving access to healthcare and education in low-income communities. However, we can't ignore the downsides of AI's growth. Human rights are jeopardized by AI systems' inherent biases and discriminatory acts, which further entrench existing inequalities. In addition, there are valid concerns regarding privacy and data security due to the persistent pursuit of data-based insights. There is a greater risk of exploitation and increasing monitoring as AI systems gather vast amounts of personal data. Deep Fakes, privacy breaches, AI prejudice and discrimination, and other examples of AI misuse have presented AI-driven difficulties.[1]

The term "personality rights" describes the entitlement to have one's unique qualities and worth upheld by the law. It includes the freedom to pursue one's own interests in a way that is consistent with one's unique personality, to safeguard one's identity, and to avoid any distortion of that identity. A person's honour, privacy, and dignity are protected by these rights. Unauthorized use of a person's likeness or persona for financial benefit is a common way that these rights are violated. Such exploitation of an individual's resemblance or character has become very easy and familiar with the introduction of AI technology, which poses a more substantial danger to personality rights. Concerns about people's agency over their own identities are exacerbated by the commercial exploitation of user-generated material by AI systems. Unauthorized use of a person's voice and likeness is possible with technologies like deepfake films and artificial speech synthesis, which can lead to deceptive portrayals. Some worry that AI voices might be used without permission or infringe on

[1] P. Nema, Understanding Copyright Issues Entailing Deepfakes in India, 29 INDIAN J.L. & TECH. 241, 245 (2021).

Indian Journal of Law and Jurisprudence | Licensed under Creative Commons — https://creativecommons.org/licenses/by/4.0/ | DOI: 10.5281/zenodo.24207333 | Title: Deepfake and Personality Rights: An Emerging Cyber-IPR Conflict

people's personality rights because of this capability. There is a risk of unintentional exploitation since people do not have control over how AI systems use personal data, which includes voice and picture.

Deepfakes and AI-generated avatars can steal performers' likenesses and utilize them without their agreement, threatening their personality rights. Deepfakes and AI human copies threaten consumer rights by making deception and manipulation simpler. These technologies can misrepresent reputations or deceive people into illicit financial transactions. Such approaches damage consumer's confidence, especially in increasingly digitized countries like India, where different marketplaces and varying digital literacy make customers more vulnerable. To solve these problems, intellectual property rights (IPR) legislation must be reevaluated, a licensing structure tailored to AI systems must be developed, and ethical standards must be established to protect creators while encouraging research. There has to be protection in place to prevent the fast development and impact of AI from outpacing the ability of legal institutions to handle its consequences. Otherwise, there will be confusion and disputes in the world of intellectual property.[2]

2. DEEPFAKES AND THE EVOLVING LEGAL LANDSCAPE OF PRIVACY IDENTITY AND PERSONALITY RIGHTS

2.1 Deepfake Technology and the Emerging Legal Challenges to Privacy, Identity, and Digital Authenticity

Among the most significant advancements in the digital realm in this age of lightning-fast technical advancement is deepfake technology. The line between reality and fiction may be blurred with the use of deepfake technology, which creates movies, audio files, and photographs using artificial intelligence. This development of synthetic media has allowed for the fabrication of people who have never done or said anything before, with or without their knowledge or permission. The technical steps that made this possible began as a joke but have since raised serious moral, legal, and societal questions. Despite the fact that deepfakes have both good and bad uses, such as in creative, satire, or parody works, they have also been used maliciously. It manifests itself in a variety of ways, including the creation of misleading videos for political purposes, the dissemination of false information, the slander of persons, and the publishing of explicit content without the owners' permission. Deepfake technology's

[2] PAVAN DUGGAL, ARTIFICIAL INTELLIGENCE LAW AND REGULATION IN INDIA 124 (Cyberlaw University 2021).

accessibility poses a serious, pervasive danger to rights to privacy, identity, and reputation, which are guaranteed by several international constitutions.

Deepfakes may be seen as an attack on personality, which can affect image and likeness rights. These technologies threaten privacy, security, and legal rights as they spread. Deepfakes have been used to impersonate celebrities, manipulate elections, and utilize them without their consent.

Current legal frameworks don't always capture the intricacy of deep fake technologies when it comes to unlawful use of another's image, likeness, or voice. During the 2020 Delhi Legislative Assembly elections, a deepfake video of BJP politician Manoj Tiwari went viral, causing political confusion.

Similarly, in the case of "*Lindsay Lohan v. Take-Two Interactive Software, Inc. (2013)*",[3] significant questions about online privacy were raised when a video game appropriated an individual's appearance. The seriousness of these incidents highlights the need for a comprehensive legal response to deepfakes in order to forestall their malicious application.

Recent high-profile cases have shown that deepfake technology raises serious legal issues. Deep fake films in political campaigns can easily manipulate public opinion and undermine democracy, as shown by the Manoj Tiwari incident in India. Like Lindsay Lohan, other celebrities have sued companies that use their likenesses in deepfake films without permission.

Due to deepfake technology, the legal community may have trouble distinguishing real from fake material. A rise in deepfake defence strategies, such as claiming evidence is a deep fake, could cast doubt on digital evidence and slow down the legal process. As AI-based technologies like deepfakes become more complex, legislative authorities worldwide are under pressure to revise copyright and personality rights laws. These reforms must strike a balance between individual rights and free speech to ensure that the relevant legal system is unprepared for AI technology.[4]

IJLJ
ISSN: 2583-2794

2.2 Deepfakes, Personality Rights, and the Emerging Legal Framework for Digital Identity Protection in India

One of the most divisive technological developments of the modern period is deepfake. It is possible for AI-generated media manipulations to alter audio recordings, movies, and photographs in order to give the impression that they are legitimate, when in fact they are

[3] 2018 NY Slip Op 02208.
[4] Chintan Pathak, Impact of Deepfake Technology on Indian Society, 5 VIVEKANANDA TECH. & L. REV. 112, 118 (2023).

entirely synthetic. Despite initial excitement in deepfakes as a creative tool, its unchecked use has become a major problem in the realm of copyright and personality rights infringements. The original author retains full ownership of his work and all rights to copy, distribute, and perform it publicly under copyright law. Deepfakes subvert these standards by enabling unauthorized use of copyrighted materials, such as an actor's likeness or a public figure's voice. The dilemma that arises is who owns the rights of the person to their digital likeness, given that deepfakes may be used to generate an extremely exact replica of their likeness or even their voice.

Although AI's meteoric rise has ushered in a plethora of new possibilities, it has also paved the way for deepfakes, the greatest identity danger of our day. Deepfakes mimic the appearance and sound of a real person by using artificial intelligence to create convincing video or picture replacements. When well-known people discover that their likenesses, voices, or features have been utilized without their consent, what began as a harmless online fad becomes a major ethical and legal concern. Under the growing umbrella of personality rights, Indian courts are starting to give this serious consideration.

Subject to the restrictions outlined in Article 19(2), the right to freedom of speech and expression is guaranteed to all people by Article 19(1)(a) of the Constitution. State security, Bharat's sovereignty and integrity, friendly relations with foreign states, public order, decency or morality, contempt of court, defamation, and incitement to an offence are all reasons that the State may reasonably restrict free speech and expression under Article 19(2). The Supreme Court's decision in "*K.S. Puttaswamy v. Union of India*" established that the right to privacy, including the right to one's personal information, is a crucial component of the right to life and liberty as provided by Article 21 of the Constitution. It was noted by the Court:

"*The dangers to privacy in an age of information can originate not only from the State but from non-state actors as well. We commend the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the State. The legitimate aims of the State would include, for instance, protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits.*"[5]

As, the IT Act targets cybercrimes such as identity theft and the transfer of pornographic content via computer means. The impact of these crimes on society has been exacerbated by deepfake, which has made their conduct easier but more difficult to detect. The current system

[5] 2019 (1) SCC 1.

established by the IT Act may be depended upon to deter deepfake-related cybercrimes, but no such framework now exists.

For instance, in a government advisory on the "IT Act, 2000 and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", the Indian government outlined the standards for due diligence that platforms and intermediaries must meet. One of the requirements is that any synthetic media that an intermediary allows, even if it could be used for deepfake or misinformation, must be marked with a unique identifier or metadata that shows that it was created, generated, or altered using the intermediary's computer resources.

In a future when flawless facial and vocal replicas are within reach of technology, the next question is how far the law may go to safeguard an individual's identity. Although personality rights have developed by judicial interpretation, they are not explicitly stated in any Indian legislation. Article 21 of the Constitution guarantees an individual's right to privacy, and these rights are related to the right to publicity, which enables an individual to manage the economic use of their likeness and identity. Personality rights safeguard the monetary worth of public personalities and celebrities in addition to their individual identities. Infringing on a famous person's privacy and economic interest occurs when their picture is used for commercial purposes without their consent.

But deepfakes are more difficult to combat since their creators aren't necessarily looking to make a profit. Intentional political satire or even harmful disinformation is the goal of many. In the landmark case of "*Amitabh Bachchan v. Rajat Nagi & Ors*",[6] which took place in 2024, the Delhi High Court handed down a significant ruling about this matter. In this case, the renowned actor had sought redress for the unlawful use of his image, voice, and identity in deceptive promotional materials.

The court ruled that famous people have an inherent right to manage the use of their likeness and likeness alone. According to the judge, deepfake technology may deceive the public and damage people's reputations, particularly when the video is so convincingly fake that nobody can tell it's not genuine. A temporary restraining order was issued by the court, prohibiting the unlicensed use of Mr. Bachchan's likeness, voice, or image. Many more famous people have submitted such petitions since then.

After discovering AI-generated films of themselves promoting businesses or making words they never really uttered, stars including Hrithik Roshan, Katrina Kaif, and Anil Kapoor sued the Delhi High Court in 2025. This kind of exploitation infringes on their personality rights and, according to the court, might be considered passing off, misappropriation, or even

[6] (2022) 6 HCC (Del) 641.

defamation. The courts are seeing deepfake usage as a type of intellectual property violation in these particular circumstances, in addition to being a morally reprehensible thing to do, because it entails the unauthorized use of a person's identifying traits, which have commercial worth. Indian law is gradually adjusting to the digital realm, as seen by the aggressive position of the Delhi High Court. Nevertheless, no all-encompassing law has been passed that deals with deepfakes or personality rights.

Personal information is exempt from copyright protection under the Copyright Act. Brand names and logos are protected by the Trade Marks Act, but faces and voices are not. While cybercrime and data misuse are addressed in the Information Technology Act, AI-powered identity cloning is not. Because of this loophole in the law, victims of deepfakes who aren't well-known enough to get court attention have a hard time getting their cases resolved quickly and effectively. At this juncture, the anticipated replacement of the present IT Act by the Digital India Bill takes of paramount importance. It has been discussed in draft form and may contain measures to safeguard digital identities and punish the abuse of AI-generated material. By addressing concerns about privacy and authenticity while still protecting the right to free speech, this framework has the potential to become the first of its kind in India regarding the regulation of deepfakes.[7]

Following in the footsteps of the European Union's Artificial Intelligence Act, which mandates disclosure of the use of synthetic media, the Bill may impose duties on content providers and social media platforms to either remove or identify AI-generated material.

If everyone could control their online voice and face, Instagram, TikTok, and YouTube would have huge compliance requirements. Excessive limitation may impede free expression, satire, and creativity. The same legal framework that targets dangerous deepfakes may also catch comedians who parody politicians or artists who use AI to attack celebrity culture. Politicians struggle to find that balance.

When technology can duplicate your voice or appearance, identity becomes intellectual property. Law students will find this topic powerful, combining constitutional rights, intellectual property, and cyber law. This shows that courts are actively protecting people against abuse by repurposing concepts rather than waiting for Parliament to act. The Delhi High Court prioritises human dignity. Courts weigh economic damage and individual sovereignty.[8]

[7] KARNIKA SETH, COMPUTERS, INTERNET AND NEW TECHNOLOGY LAWS 178 (2d ed. LexisNexis 2017).

[8] Biranchi Narayan P. Panda & Isha Sharma, Deepfake Technology in India and World: Foreboding and Forbidding, 6 ASIAN INST. RES. J.L. & HUM. RTS. 55, 60 (2022).

No one should ever lose the freedom to choose their own public representation just because technology advances. This approach is in line with the worldwide trend observed in places like the EU, where privacy laws offer robust protections against digital impersonation, and the US, where states like California have passed particular "right of publicity" laws that protect individuals from the unauthorized use of their likenesses. India will need to clarify its regulations on the production and dissemination of deepfakes in the coming years. Legislation is necessary for substantive change, while the courts can only interpret laws. There will be even less differentiation between real and artificial as AI finds greater uses in entertainment and social media. Legislators must create frameworks that protect truth, consent, and creativity. Discussion of deepfakes and personality rights is the current intellectual property frontier. In an age of digital reproduction, identity ownership is the issue, not patents or trademarks.[9]

3. DEEPFAKE TECHNOLOGY AND ITS LEGAL, ETHICAL, AND SOCIO-ECONOMIC IMPLICATIONS IN THE AI-DRIVEN WORLD

3.1 Privacy, Identity, and Accountability in the AI Era

The proliferation of deepfake technology, propelled by advancements in AI and ML, presents complex compliance and regulatory challenges globally, with particular consequences for India. "Deepfakes" is a combination of "deep learning" and "fake" used to describe the processing of genuine photographs. Unauthorized changes to voices and facial expressions are not uncommon. Their cutting-edge AI, ML, and deep learning capabilities should give you a good idea of how far it goes. The potential for abuse of these technologies is a valid worry. Digital processing of various media files, such as audio, video, and picture data, is done using artificial intelligence to generate deep images. Organizational trust, individual reputations, and the veracity of claims can all be eroded by digitally controlled media. Furthermore, new questions about responsibility, jurisdiction, and the level of protection offered to persons and companies arise as a result of the merging of deepfake technology with existing legal frameworks, such as those pertaining to privacy, intellectual property, defamation, and others. As things are, there are no country-specific rules in India, but the present dangers necessitate a stronger and more flexible legal framework, and the Indian government has admitted that this is happening.

[9] TALAT FATIMA, CYBER CRIMES 142 (Eastern Book Company 2016).

Even after trying new things, deepfake continues to cause problems on a worldwide scale. Case in point: in the US, several states have passed laws concerning the production and dissemination of deepfakes, especially those employed in political campaigns or for the production of non-consensual pornography. Much as in the United States, the European Union is actively working on laws that would regulate AI in its whole, including deepfake. A bigger human verification remains a vital phase in the information verification process, despite the fact that several jurisdictions have aggressively sought out current technological solutions to tackle deepfakes.

There are potential legal, social, economic, and political repercussions to the production and dissemination of deepfakes. Worldwide, lawmakers and law enforcement agencies are facing a major challenge from deepfake technology, which has progressed at a faster rate than regulatory and legal frameworks. Deepfakes can be used for propaganda, non-consensual pornography, and financial market manipulation. AI law must address deepfakes, biased algorithms, and data security. The opaque nature of AI decision-making raises concerns about responsibility and unintended repercussions.

Data protection, information technology, and defamation laws in India may apply, but they are not designed to handle deepfakes. The country's legal structure for such instances is changing. Deepfakes are not specifically addressed by Indian law, thus a more sophisticated technique is needed to avoid misunderstandings and protection gaps. Additionally, India's legal system has yet to handle deepfakes and AI-related crimes. Government recognizes the need for regulation, but legislation is still being drafted.[10]

3.2 Misuse of Deepfake Technology Across Political, Social, and Financial Domains

An anonymous Reddit user allegedly used an open-source AI-driven application in 2017 to generate sexual material by superimposing the faces of celebrities on the bodies of regular individuals. This is the first known instance of deepfake technology in operation. For a long time, there have been editing applications like Photoshop. Thanks to the capacity to produce deepfakes, even anyone without a lot of training can manipulate audiovisual recordings and images. In 2020, the Deep Trust Alliance—a group of corporate and civil society stakeholders—issued a notice highlighting the fact that tools for creating and disseminating misinformation are now more accessible, cheaper, faster, and simpler to use. To make deepfakes, digital media including audio, video, and photos are edited and modified using

[10] Vidya Vinutha Dsouza & Glavin Dsouza, Deepfakes and Their Ethical Implications, 12 INT'L J. INNOVATIVE RES. & TECH. 3388, 3392 (2024).

artificial intelligence (AI). Given their use of hyper-realistic digital fabrication, they may be used to fabricate evidence, damage reputations, and undermine faith in democratic institutions. The political damage, reputational damage, and financial damage caused by deepfakes are the three main categories into which these falsehoods fall.

With the help of Deepfake, an Indian politician working for the BJP was able to change his earlier speech about the "Citizen Amendment Act" into a new fake speech about the Delhi Elections. To alter the meaning of the speech, AI technology was employed. The speech was spoken in Haryanvi after it had been delivered in Hindi so that it may be heard by the electorate of Haryana.

A neutral advocacy group called "RepresentUs" was behind the fabrication of Deepfakes of Russia's president, Vladimir Putin. It was the original intent of the creators of the DeepFakes of Kim Jong-un and Vladimir Putin to air as ads during the US elections, shocking American citizens into realising how fragile their democracy is and showing how the media can shape a nation's destiny whatever their credibility level.[11]

The Indian star Ranveer Singh has taken legal action after a deepfake video claiming he supports a political party went viral. The interview he gave to the news agency ANI while in Varanasi is real, and you can watch it in the video. But artificial intelligence was used to create the soundtrack. The deepfake video showed Ranveer Singh criticizing Prime Minister Narendra Modi's policies on inflation and unemployment. The final touches to the polished film were messages asking people to vote for the Congress. The legal team defending Ranveer Singh has confirmed that an investigation into the case has begun following the filing of a FIR. He cautioned his Instagram followers, "Friends, beware of deepfakes," after the deepfake went viral.

With over 2.4 million views, a deepfake video starring Rashmika Mandanna has become incredibly popular. Rashmika Mandana, an actor from India, was lately the victim of deepfake technology, a particularly sinister kind of cyberbullying. Artificial intelligence (AI) "deep fakes" use "deep learning" with inaccurate data to generate realistic-looking portraits of real people; these portraits may be nearly indistinguishable from one another. Deepfake photographs may be a useful technique for altering someone's online persona, whether you have their consent or not. This encompasses changing features like hair length, skin tone, etc., as well as changing faces. Internet users should be cognizant of the grave dangers posed by artificial intelligence, despite the fact that it is hard to deny the incredible progress this technology has achieved in recent times. As instances of online harassment and abuse,

[11] V.K. AHUJA, LAW RELATING TO INTELLECTUAL PROPERTY RIGHTS 389 (3d ed. LexisNexis 2017).

including the disclosure or threat of disclosure of deepfake images of persons, have increased, the availability of legal protections against these photos has come under investigation.

A Deepfake video with Barack Obama insulting and slurs Donald Trump was uploaded on YouTube on April 17th, 2018. This Deepfake teaser was created and produced by BuzzFeed and Monkeypaw Productions in collaboration with American actor Jordan Peele. It was the intention of this video to shed light on the extremely dangerous consequences and power of Deepkakes, which have the ability to influence anyone to say anything.[12]

In 2019, for example, a UK-based energy company's CEO thought he was on the phone with his boss, the CEO of the firm's German parent company, and proceeded to transfer €220,000 (about $243,000) to a Hungarian supplier's bank account, all because deepfakes had the potential to cause enormous financial losses. It turned out that the voice belonged to a criminal who had fabricated the CEO's voice using AI voice modification technology. It was one of the earliest examples of using AI to compose music that sounded like a genuine voice.

During a video chat with their deepfake colleagues, one Hong Kong finance worker was tricked into giving out $25 million. Carefully mimicking real people's activities, the deepfake personas made the deception easier to pull off. The employee learned of the lie only after he or she contacted corporate headquarters.

A new set of concerns and difficulties for regulators has emerged as a consequence of the spread of deepfakes. In order to set limits on the use of technology while balancing the interests of digital companies, creative industries, healthcare, consumers, and others, regulators must move quickly. Since they often work anonymously, adapt quickly, and disseminate their synthetic creations over international internet platforms, catching the most dangerous individuals is one of the toughest issues in enforcement. Since deepfakes can spread false or misleading information, they pose a threat to free speech generally and political speech in particular.[13]

4. GLOBLAL APPROACHES AGAINST DEEPFAKE AND PERSONALITY RIGHTS

There has been a marked increase in the global recognition of the need for comprehensive deepfake regulation. A number of global bodies have started debating the best way to regulate technology in a way that safeguards victims, including the UN and the World Economic Forum. The importance of preserving innovation and free speech while preventing damage is brought to light in these discussions. Congress has to do something about the risks posed by

[12] L. Dami, Analysis of Deepfake Technology as a Cyber Threat, 9 INT'L J. EMERGING TECH. & INNOVATIVE RES. 75, 79 (2022).
[13] *Ibid*.

deep-diving technology, which makes phoney films and pictures (sometimes dubbed "deepfakes").

Disclosure of the usage of deep-sea imagery in films and other media is now mandatory according to new laws announced by the Chinese government in 2019. Further, these regulations forbid the dissemination of deep material in the absence of an obvious and unmistakable sign that it is artificial. Furthermore, on “January 10, 2023, the Cyberspace Administration of China (CAC)” laws governing tech developers will be put into effect by the Chinese government. Those responsible for making and using development regulations and advertising are equally responsible for all parts of them. Businesses and individuals using deep processing systems have various responsibilities, such as obtaining consent, verifying identities, registering information with the government, reporting illegal content, setting denials, processing refunds, and fulfilling other obligations. Here we see China's forward-thinking strategy for handling the dangers posed by AI and deepfake.[14]

The anti-fraud laws in Canada are built around three interconnected pillars: detection, response, and prevention. The Canadian government is making great strides to educate the public about important technology and provide preventative systems to curb the occurrence and spread of fraud. The government is currently contemplating passing legislation to prohibit the distribution or usage of leather in order to do this, which is considered illegal. It is now against the law in Canada to share someone else's private photo without their consent.

The Canadian Elections Act has provisions that may be applicable to deepfake, much to the California Elections Act. "Safeguard Canada's 2019 election" and the "Critical Election Incident Public Protocol," a panel inquiry mechanism for deepfake occurrences, are two more measures that Canada has recently implemented to mitigate the ill impacts of deepfakes. The Canadian government has taken both of these steps as part of its strategy to reduce emissions. Many, however, maintain that Canada still lacks an adequate system to deal with deepfake threats.

South Korea was an early investor in artificial intelligence research and regulatory study, which makes sense given the country's remarkable technical achievements. Over the next five years, the South Korean government would invest one trillion won (about $750 million USD) toward AI research, according to an announcement made in January 2016. The South Korean government unveiled their AI strategy in December 2019.[15]

[14] NISHITH DESAI ASSOCS., ARTIFICIAL INTELLIGENCE: REGULATORY AND POLICY FRAMEWORK IN INDIA 78 (Nishith Desai Associates 2020).

[15] R. Singh & A. Verma, Deepfakes and the Challenge to Privacy and Data Protection in India, 8 INDIAN J. LAW & JUST. 201, 207 (2023).

South Korea decriminalised the dissemination of deep fakes that could "cause harm to public interest" in 2020 when a new law was passed. Violators face penalties of up to fifty million won (about $43,000) in fines or five years in jail, depending on the severity of the offence. Protesters are urging South Korea to do more to combat sexual offences and online pornography by increasing funding for programs that educate the public, provide civil remedies, and establish redress.

When faced with AI technology, the United States was quick to respond. Legislation defining the term "Deepfake" was first passed by the United States Congress in December 2018 with the passing of the "Malicious Deep Fake Prohibition Act of 2018" (S. 3805, 2023). It wasn't until June 2019 that the "Deepfakes Accountability Act" was mentioned. Still, many are worried that it would be in conflict with the First Amendment and that its vague wording will lead to public outcry. This year, lawmakers proposed the "Deepfake Report Act" to require the DHS to release evaluation reports on deepfake technology at regular intervals. In addition, certain countries move swiftly to deal with cases of "deepfake" abuse, especially when it comes to pornographic movies and election campaigns.

Concerning the emerging technology of deepfake, only a few of US states have passed laws. California passed AB730 in 2018 and Texas ratified S.B. 751. These two rules make it illegal to use deepfakes, which might influence the next election.

Virginia's Senate Bill 1736, Georgia's Senate Bill 337, and California's AB602 all aim to ban the creation and dissemination of non-consensual deepfake pornography. Individuals now have the legal recourse to sue those responsible for the illegal dissemination of deepfakes, according to New York statute S6829A passed in 2020. Numerous state legislatures have recently filed and approved a slew of bills to regulate AI in 2022. While there have been some positive breakthroughs in AI-related US law, most states still haven't introduced or passed any comprehensive AI-specific legislation.[16]

European Union legislation pertaining to "deepfake" technology was initially lacking. Nevertheless, they have brought 'deepfake' into their regulatory purview through a series of rules and programs. The goal of these steps is to limit the use of deepfakes in domains including regulating AI, protecting personal information, and fighting misinformation.

The Artificial Intelligence Policy of the European Union is one of the earliest attempts to control AI on a worldwide scale. The document's stated goal is to provide uniform regulations for IP creation, commercialization, and usage throughout the European Union in an effort to transform the bloc into a trusted center for IP. A secure and welcoming workplace that

[16] GAUTAM BHATIA, THE TRANSFORMATIVE CONSTITUTION 201 (HarperCollins 2019).

upholds and defends the basic rights and ethical principles of all persons is the declared goal of the directive, which should be implemented by all EU AI systems. The law's primary goals are to (a) encourage investment and innovation in IP-related fields, (b) fortify IP and governance, and (c) provide conditions for the development of EU-wide business intelligence. The Artificial Intelligence Act incorporates a number of EU statutes governing different sectors of the digital economy, together with the Data Protection Act, the Digital Services Act, and the Digital Economy Act. However, the Artificial Intelligence Bill makes no direct mention of data security, internet platforms, or content settings.

5. REGULATORY GAPS AND EMERGING SAFEGUARDS IN INDIA'S APPROACH TO DEEPFAKES

5.1 Legal Framework Governing Deepfakes and AI-Enabled Cybercrimes in India

India does not have a law that directly addresses deepfakes or crimes linked to artificial intelligence, although there are sections in many statutes that might lead to criminal and civil penalties.

Invading someone's private by taking, publishing, or publishing it in the mainstream media is considered fraud. For offences like this, see Section 66E of the IT Act. A fine of two lakhs or three years in jail is the maximum penalty. Also, systems that generate deep connections are part of the unauthorized computer access that is dealt with under Section 43 of the Information Technology Act, 2000. According to Section 66D of the IT Act, anybody who utilizes modern technology to defraud or impersonate another person is subject to punishment. The maximum penalty for this is three years in prison and/or one million rupees in fines.

The power to prosecute individuals who distribute deepfake content containing explicit or obscene sexual content is granted under Sections 67, 67A, and 67B on Obscene Content of the IT Act. The failure to promptly remove "artificially morphed images" poses a threat to the "safe harbour" protections enjoyed by social media corporations.[17]

"Information Technology [Instructions to Intermediaries (Amendment) Rules, 2018]" is the revised policy that the Department of Electronics and Information Technology has released. The "Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 for an Open, Safe & Trusted and Accountable Internet, 2023" mandate that, upon receiving a complaint, intermediaries must either delete or disable

[17] S. K. Sharma, Regulating Artificial Intelligence and Deepfakes: An Indian Perspective, 4 NLU DELHI L. & TECH. REV. 67, 73 (2022).

access to unlawful data within one hour. It can help you overcome long-standing limitations in India.

In view of the rapid development of cybercrime-related technologies, the Bharatiya Nyaya Sanhita (BNS) has strict rules for dealing with such offences. Regardless of medium, Section 294 makes it illegal to publish or transmit pornographic material. Penalties for violations include fines and jail time, with harsher consequences for recurrent offenders. The unlicensed taking or distribution of pictures of a woman's private parts or activities is called voyeurism and is addressed under Section 77.

Theft of digital assets, such as data or money obtained through online techniques, is also dealt with under Section 316. Offences such email spoofing and internet forgeries are addressed under Sections 336, 354, and 356. Both the act of defamation itself and the dissemination of such material by electronic mail or any other digital means are punishable under these clauses. Imprisonment and fines are imposed by it. Section 111 and other sections deal with Organised Crime, which includes gang-perpetrated cybercrimes including data trafficking and online frauds.[18]

If it is illegal to produce copies of the content, then Copyright 1957 may apply. If someone owns exclusive rights over anything, it's against the law to utilize that content without their consent. This offers a legitimate solution to address the illicit matters about deepfakes.

At the moment, India is experiencing the age of hyper-realistic AI, or "deepfake," which presents unique difficulties for our legal and ethical frameworks. While deepfakes might revolutionise narrative and entertainment, their misuse could lead to major problems with privacy, human rights, and the veracity of information.

5.2 India’s Emerging Response to AI Deepfake Misuse

The business sector's role in implementing safeguards, some of which are also large investors in artificial intelligence, is crucial. Along with advocating for the development of ethical AI, Google is now in talks with the Indian government to set up a "multi-stakeholder discussion" to tackle the challenges of dealing with deepfaked material. Also, a think tank aimed at creating guidelines for the moral use of AI was formed by a partnership between Google and the Indian Institute of Technology, Chennai.

Ironically, the use of deepfakes in illegal activities has been limited by the Indian judiciary. The well-known Indian actor "Anil Kapoor" has now asked for a ban on the use of his

[18] APAR GUPTA, DIGITAL FREEDOM IN INDIA: CONSTITUTIONAL PERSPECTIVES 96 (Internet Freedom Foundation 2020).

likeness, voice, identity, publicity, and other characteristics on the internet. The defendants used artificial intelligence deepfake technology to create offensive content with Mr. Kapoor's likeness, personality traits, and movie-related terms superimposed over the bodies of famous people in order to market their wares.

An injunction banning the defendants from employing any kind of machine learning, artificial intelligence, deepfakes, or face morphing in relation to Mr. Kapoor's name, likeness, voice, personality, etc., whether for financial gain or otherwise, was warranted by the actors' argument. The actor has suffered irreparable harm, including social, economic, and/or the violation of his right to a decent existence, as well as prima facie proof of the unlawful use of his image, photograph, and other information. These kinds of reliefs have long been present throughout India. When Mr. Amitabh Bachchan's fame and public persona were used to promote products in 2022, he also received similar treatment.[19]

Special Copyright Restrictions for Deepfake Technology Management are enforced to protect individuals' financial interests in the monetization of their creative production, copyright rights are often provided.

In India, there are presently no regulations that control the use of AI. This openness has been fantastic for AI advancements as anybody with access to tools like ChatGPT or Mid Trip may use them freely and without fear of repercussions. Many new regulations have been put into place throughout the previous five years. Among these, Niti Ayog's 2018 National AI Strategy (#AIFORALL) and the Principles of Responsible AI (2020) were announced. The Digital Personal Data Protection (DPDP) Act, which governs the processing of digital personal data in India, was also introduced by the government in 2023. On the other hand, these regulations stress the importance of AI's data usage and the ways in which different industries gain from AI-enabled resources. There are currently no regulations in place that forbid the consumer-level exploitation of AI, including the utilization of voice samples, photographs, or videos.

6. CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

With the use of AI, identity theft has become more sophisticated, with tactics such as cloned celebrity voices and false social media profiles. Indian courts are beginning to acknowledge personality rights as a vital legal protection against the exploitation of a person's name, voice,

[19] Ananya Chatterjee, Deepfakes, Democracy and Misinformation: A Socio-Legal Analysis, 10 J. MEDIA L. & ETHICS 145, 150 (2024).

face, and reputation in the age of digital tools that make it possible to create deepfake videos that look and sound very realistic, clone faces in a matter of seconds, and more.

The lines between reality and digital fabrication have become more blurry as a result of technological breakthroughs that have made it easier than ever to replicate an individual's identity. In light of this, personality rights are quickly becoming a landmark piece of Indian legislation.

A person's identity, which includes their name, likeness, voice, and other unique traits, is being more and more acknowledged by courts across as having legal and commercial significance. Both reputational damage and significant financial loss can occur from the unlawful use or exploitation of these features. Thus, in order to prevent individuals' identities from being misused in the ever-growing digital realm, Indian legislation is progressively coming to support personality rights.

It is evident from the preceding discussion that no jurisdiction, including India, follows such comprehensive legislation. Nevertheless, the G7 has lately published a set of guidelines for groups interested in advanced AI systems, with the goal of promoting trust, security, and safety in AI research and development. Duality is demonstrated by Deepfake technology in the realm of artificial intelligence.

Having worries and negative emotions regarding abuse while having pleasant times and good sentiments brings up significant questions. Staying alert and coming up with ways to limit harm are crucial as deepfake algorithms keep becoming better. To finish the difficult path of deep learning and preserve the digital world's integrity, security, and trust, we must increase public awareness, invest in research technologies, and pass suitable laws and regulations. Deep engagement is the source of electronic technologies' far-reaching impacts. The significance of comprehending the whole scope of technology—its procedures, capacities, and the outcomes it is capable of producing—is shown by two comprehensive instances.

Given its ubiquity, consumers and businesses must understand this technology's content and focus procedures. Information literacy, training, and evidence-based strategies are needed to succeed in this ever-changing world. Deepfakes have made it harder to tell fake material from real. Many advocacy groups have battled against personal usage, unlawful activities, fraud, obscenity, and other crimes to balance technology and public enlightenment.

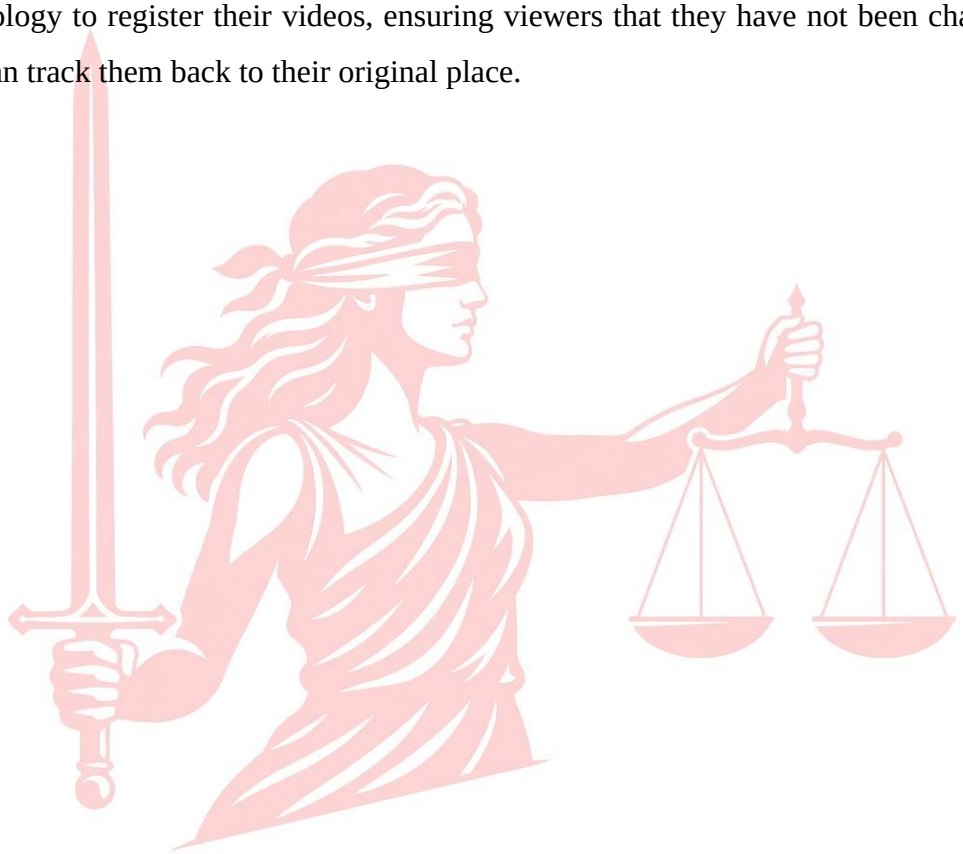
They include the Electronic Frontier Foundation, Witness Media Lab, Alliance for Content Provenance and Authenticity, and others. The controller may consider legal options to protect names, personal information, legal rights, and human rights.

6.2 Recommendations

- The creation and distribution of deepfake content that is harmful to people should be made illegal by specific laws. Based on the extent of the harm caused by the deepfake, the punishment could consist of fines alone, jail time alone, or a combination of the two.
- An improvement in the protection of rights of personality necessitates new laws that allow famous people and regular people alike to use legal action when their likeness or voice is used in a deepfake without their knowledge or consent.
- The illegal use of a person's voice or likeness in deep fake videos necessitates a change to copyright laws. Individual artists and public figures would be able to assert their online IP rights in this way.
- Their extensions are a sensible addition to security measures, since a wider use of digital manipulations like deepfakes would be to people's advantage. The rapid proliferation of deepfakes makes it difficult for current defamation laws to stay up. Due to the rapid dissemination and improvement of deepfake on social media, as well as the anonymity and speed of these technologies, the victims of their harm are often unable to hold them accountable. Any changes to the law should revolve around making it easier to identify deepfakes as defamatory content and for victims to have their claims heard.
- Also, until the matter can be permanently resolved in court, courts should be able to issue temporary injunctions to prevent further dissemination of defamatory deepfake content. Social media platforms such as Facebook, Twitter, and YouTube should be compelled to remove harmful deepfakes upon notification and collaborate with law enforcement to apprehend those responsible. Fighting the wrongful use of deepfakes should be a top priority for technology.
- AI-based detection methods are needed to identify and delete dangerous deepfake videos and photos. Some tech suppliers are developing deepfake detection systems, but they must be enhanced and applied countrywide for public safety and legal compliance.
- AI and ML may be used to detect tiny signals of deepfake material, such as lighting, face expressions, and speech production. These tools should be connected with digital networks to automatically recognise uploaded deepfakes. This speeds up intervention. An AI-powered technology from cybersecurity startup Deeptrace can identify digital content trends to authenticate deepfake films.

IJLJ — ISSN: 2583-2794

- Social media sites might use this technique to detect and eliminate deepfakes before they spread. Blockchain technology might solve this by verifying digital media.
- Blockchain technology records who modifies digital material, giving consumers and sites piece of mind that images and videos cannot be changed. This might drastically minimise deepfake concerns. Blockchain technology should be promoted by governments to secure digital media records. Video producers may utilise blockchain technology to register their videos, ensuring viewers that they have not been changed and can track them back to their original place.



— I J L J —
ISSN: 2583-2794

REFERENCES

1. P. Nema, Understanding Copyright Issues Entailing Deepfakes in India, 29 INDIAN J.L. & TECH. 241, 245 (2021).

2. PAVAN DUGGAL, ARTIFICIAL INTELLIGENCE LAW AND REGULATION IN INDIA 124 (Cyberlaw University 2021).

3. Chintan Pathak, Impact of Deepfake Technology on Indian Society, 5 VIVEKANANDA TECH. & L. REV. 112, 118 (2023).

4. KARNIKA SETH, COMPUTERS, INTERNET AND NEW TECHNOLOGY LAWS 178 (2d ed. LexisNexis 2017).

5. Biranchi Narayan P. Panda & Isha Sharma, Deepfake Technology in India and World: Foreboding and Forbidding, 6 ASIAN INST. RES. J.L. & HUM. RTS. 55, 60 (2022).

6. TALAT FATIMA, CYBER CRIMES 142 (Eastern Book Company 2016).

7. Vidya Vinutha Dsouza & Glavin Dsouza, Deepfakes and Their Ethical Implications, 12 INT'L J. INNOVATIVE RES. & TECH. 3388, 3392 (2024).

8. V.K. AHUJA, LAW RELATING TO INTELLECTUAL PROPERTY RIGHTS 389 (3d ed. LexisNexis 2017).

9. L. Dami, Analysis of Deepfake Technology as a Cyber Threat, 9 INT'L J. EMERGING TECH. & INNOVATIVE RES. 75, 79 (2022).

10. NISHITH DESAI ASSOCS., ARTIFICIAL INTELLIGENCE: REGULATORY AND POLICY FRAMEWORK IN INDIA 78 (Nishith Desai Associates 2020).

11. R. Singh & A. Verma, Deepfakes and the Challenge to Privacy and Data Protection in India, 8 INDIAN J. LAW & JUST. 201, 207 (2023).

12. GAUTAM BHATIA, THE TRANSFORMATIVE CONSTITUTION 201 (HarperCollins 2019).

13. S. K. Sharma, Regulating Artificial Intelligence and Deepfakes: An Indian Perspective, 4 NLU DELHI L. & TECH. REV. 67, 73 (2022).

14. APAR GUPTA, DIGITAL FREEDOM IN INDIA: CONSTITUTIONAL PERSPECTIVES 96 (Internet Freedom Foundation 2020).

15. Ananya Chatterjee, Deepfakes, Democracy and Misinformation: A Socio-Legal Analysis, 10 J. MEDIA L. & ETHICS 145, 150 (2024).