CONSTITUTIONAL QUANDARY FROM FIREWALLS TO FREEDOMS: THE ROLE OF IPR IN PICKETING AGAINST DEEPFAKE EXPLOITATION IN INDIA

Ruprekha Chatterjee & Madhurima De, Shyambazar Law College, Calcutta University

ABSTRACT

Today in this century there's no space for doubt regarding rapid yield of deepfake technology from a novelty to a powerful tool of manipulation, that is hoisting urgent concerns for individual rights, public trust, and legal enforcement. These AI-birthed synthetic videos and images time an again indistinct from actual content have been increasingly operated to harass, impersonate, defame, and exploit individuals, in a country like India, where legal safeguards remain fragmented and reactive in practice. As such, deepfakes dare not just technological regulation but the very foundations of constitutional aegis, including the right to privacy, dignity, and free expression. This paper will portray the triangular interplay between deepfake exploitation, Intellectual Property Rights (IPR), and the Indian Constitution. It will scrutinize whether and how the IPR laws in force specially, those protecting copyright, trademarks, and moral rights augmenting meaningful protection to individuals whose likeness, voice, or persona is malused in digital forgeries. The limitations of these laws when applied to non-commercial, non-consensual harms that fall outside traditional IPR frameworks are also being interrogated by thorough probing. Consequently, the paper will underscore the pressing need for India's legal framework to formally acknowledge personality rights and digital identity as integral to an individual's dignity, autonomy, and evolving presence in a connected world. Positioned within the larger constitutional context, the paper lights on the state's responsibility in building legal firewalls against emerging technologies while conserving the freedoms under Articles 19 and 21. Drawing from key judgments like Justice K.S. Puttaswamy v. Union of India, it emphasizes the need for a nuanced legal approach-one that integrates IPR tools with constitutional protections and cybercrime enforcement. The paper concludes that while IPR alone cannot resolve in its totality the obstacles posed by deepfakes, it can become a critical part of a hybrid legal framework anchored in constitutional values that safeguards not only creative works but the very identities and freedoms of individuals in the digital era.

Keywords: Intellectual Property Rights, Deepfake Technology, Privacy.

I. INTRODUCTION

Today in tech world it is real that all that glitters are not gold. The term Deepfake is one of the most unnerving discoveries in artificial intelligence as it is combined by two words "deep learning" and "fake". The steering mishandled media where a person's entire likeness is persuasively swayed is the soul of deepfakes. Powerful algorithms like Generative Adversarial Networks (GANs) that pit two neural networks against each other, can accomplish this task swiftly where one generates fake content, and the other evaluates its authenticity. Over time, this toil results in increasingly indistinguishable from real-life footage.[1]

In 2017, the practice of people superimposing the faces of celebrities over sexual video content initially appeared on Reddit forums and catching on like wildfire. Back then, deepfakes were all the fury for use in entertainment and applications. The art of imitation, though it started off innocently enough, has now become a powerful tool for manipulation.[2] A manipulated video can show a politician making inflammatory statements, a woman in an intimate position she never consented to, or a public figure endorsing products they never used. Society seeks answers because these aren't harmless jokes; they are violations of identity.[3] Personal privacy, reputation, democracy, and even national security are all at risk. It is really disturbing to see the exponential rise of deepfake material throughout the world. In 2019, merely 7,964 deepfake movies were detected online, according to a Deep Trace analysis. This figure increased by almost 1700% in only four years, reaching over 145,000 by 2023.[4] The majority of the ladies featured in these movies (over 90%) had no idea that their faces had been utilized in these pornographic recordings (96%).[5] Norton India reported in 2023 that 2 out of 3 adults in India are afraid they would be a victim of deepfake abuse. A whopping 77% of Indians polled admitted they had no idea how to tell the difference between a genuine and a phoney film.[6] With India's smartphone and internet penetration skyrocketing crossing 850 million active users these fears are not unfounded.[7] The accessibility of AI tools has made it easy for even

[1] Goodfellow and others, 'Generative Adversarial Nets' in Z Ghahramani, M Welling, C Cortes, N D Lawrence and K Q Weinberger (eds), *Advances in Neural Information Processing Systems* (NeurIPS, 2014) vol 27

[2] James Vincent, 'Deepfake Creator Says Goodbye After AI-generated Porn Gets Banned' (The Verge, 8 February 2018) <https://www.theverge.com/2018/2/8/16990076/ai-fakes-deepfakes-video-media> accessed 24 May 2025.

[3] Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107(6) *California Law Review* 1753

[4] Deeptrace, *Deepfake Detection and the Threat Landscape* (2019).

[5] Henry Ajder and others, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace 2019).

[6] NortonLifeLock, *Cyber Safety Insights Report: India Findings* (2023) <https://newsroom.gendigital.com/2023-Norton-Cyber-Safety-Insights-Report-Special-Release-Online-Creeping> accessed 24 May 2025.

[7] Telecom Regulatory Authority of India (TRAI), *Telecom Subscription Report for December 2023* (New Delhi:

amateur users to create convincing fakes with just a few clicks.[8]

A. From Ethical Concern to Legal Urgency

India has already grappled with a range of deepfake incidents, each leaving a mark not just on public discourse but also on the lives and reputations of those targeted. Circulation of AI-generated videos was at its peak during the 2020 Delhi Assembly elections, where political candidates were seen delivering speeches in multiple languages without their direct participation.[9] Although used by campaign teams with consent, these events demonstrated how easily deepfakes can enter the political space and potentially be repurposed for disinformation. Megacities like Hyderabad, Delhi and Bengaluru have registered increasing cases of cyber stalking, non-consensual pornography, and identity theft featuring deepfakes. According to the National Crime Records Bureau (NCRB), between 2020 and 2023, there has been a 20% increase in reported cybercrimes involving morphed or manipulated digital content.[10] However, cyber experts believe these figures are only the tip of the iceberg, with thousands of cases going unreported, especially among women, due to shame or fear of not being taken seriously by law enforcement.[11]A 2024 Cyber Peace Foundation report observed that 1 in 3 Indian women with an online presence have either experienced or feared the misuse of their images or voice through deepfake technology. Victims have reported devastating psychological impacts: from anxiety and depression to social withdrawal and suicidal ideation.[12] When digital self of an individual is distorted and used against soul, reclaiming control becomes emotionally exhausting and legally complicated.

India's legislation lags significantly in addressing the realities of deepfake exploitation. Although the Information Technology Act (IT Act),[13], provides some protection against cyber harassment and the dissemination of obscene information, the legislature is insufficient in addressing AI-manipulated content that exists in a grey area when it is neither explicitly sexual nor financially driven.[14] The inner turmoil of oneself eats away all green from life but laws operate against harm that is tangible and documentable. Deepfakes do not always leave

TRAI 2023).

[8] S Choudhury, 'Deepfakes in India: A Growing Concern' (India Today, 14 July 2022).

[9] S Banerjee, 'Political Deepfakes: Campaign Tool or Threat to Democracy?' (The Quint, 5 February 2020) https://www.thequint.com accessed 24 May 2025.

[10] National Crime Records Bureau (NCRB), *Crime in India 2022* (Ministry of Home Affairs 2023).

[11] CyberPeace Foundation, *Digital Harm and Deepfakes in India: 2024 Report* (New Delhi: CPF 2024).

[12] ibid.

[13] Information Technology Act , 2000

[14] R Bhatia, 'Indian IT Act and Its Gaps Against AI-generated Content' (2022) 9 Law and Technology Review 47

physical traces rather they rot you from inside causing psychological distress, reputational ruin, and social alienation-forms of harm that are difficult to quantify but profoundly damaging.[15] The complexity is the absence of a robust legal framework recognising digital identity as a fundamental right. While Article 21 of the Constitution guarantees the right to life and personal liberty and was interpreted in *Justice K.S. Puttaswamy v Union of India*[16] to include the right to privacy but legal enforcement in digital contexts remains fragmented and reactive.[17] Laws meant to address cybercrime, data protection, and intellectual property have not been harmonised to tackle the multifaceted threats posed by synthetic media.

The creamy path of stealing creativity is occluded by the Intellectual Property Rights (IPR), especially copyright and moral rights. But these laws were not designed to respond to intimate violations of personal identity or malicious impersonation that lack a commercial dimension.[18] Similarly, defamation law provides some relief but it requires proving malice and often involves long-drawn litigation, which many victims cannot afford emotionally or financially.[19] At this stage this study debuted to traverse the fiery trilogy between deepfake exploitation, IPR laws, and constitutional rights in India. It asks: Can existing legal frameworks are meaningfully applied to this new-age threat? Are Indian citizens protected under current laws if their faces, voices, or personas are used without consent? And if not, what kind of hybrid legal model combining IPR, constitutional protections, and cybercrime enforcement might offer a path forward?

In the United States, several states including California, Texas, and Virginia have passed laws criminalising non-consensual deepfakes.[20] China recently implemented regulations requiring watermarking of synthetic media.[21] As other countries in the world have begun taking steps India too needs to wake up now and must consider legal reform, not only to punish perpetrators but to affirm the dignity of individuals in the digital age. Though it is called deepfakes there is a real person who is socially maligned and whose identity has been manipulated, consent has been unheard. From teenager discovering a doctored video to a politician watching his words

[15] D Citron, 'Sexual Privacy in the Digital Age' (2019) 128 Yale Law Journal 1870
[16] Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (Supreme Court of India)
[17] ibid.
[18] M Kumar and D Verma, 'IPR and Identity Theft in Deepfake Culture: An Indian Legal Perspective' (2023) 28 Journal of Intellectual Property Rights 36.
[19] S Agarwal, 'Defamation Law in India and Deepfake Challenges' (2021) 14 Indian Journal of Cyber Law 95.
[20] *Bhatia* (n 14).
[21] Lin F, 'China's Deepfake Regulations: A Model for Digital Accountability?' (2023) 5(3) Technology Regulation Quarterly 82.

twisted to incite violence, the harm is deeply personal and socially corrosive. This chapter has unpacked many layers of deepfake misuse through the lens of technology, numbers, and real-life impact both around the world and here in India. What's become clear is that this isn't just a technical glitch in our digital age; it's a direct challenge to the core of what it means to live with dignity, to have a private life, and to speak freely. As we step into the next chapters, this study turns towards the law asking how Intellectual Property Rights, constitutional values, and thoughtful judicial engagement can come together to protect people in an increasingly synthetic and uncertain digital world.

II. Protection in the Age of Deepfakes

The regulations that made two acts in India especially concerning IPR and constitutional protections came across unprecedented try-out as deepfakes blossoms from academic novelty to a societal combination. Statutes like the Copyright Act, 1957[22], the Trade Marks Act, 1999[23], and the Indian Constitution[24] proffer piecemeal avenues for legal revise while others are silent. Yet deepfake needs coherent strategy to win frontal battle.

A. Copyright Law and the Manipulation of Original Works

Original works in the field of literary, artistic, cinematographic and musical content are under the banyan shield of the Copyright Act[25]. Deepfakes, however, do not merely infringe on traditional forms of creativity, they mimic identity itself. Where deepfake content manipulates an existing performance for example, replacing an actor's face in a copyrighted video with another person's likeness such use may qualify as an unauthorised derivative work under Section 14[26], especially if it copies "substantial parts" of the original content.[27] Further, Section 51[28] deems such reproduction without the rights holder's consent as actionable infringement. This could be relevant when a deepfake impersonates a copyrighted film character or inserts altered visuals into an existing work. However, the real tension lies where deepfakes do not

[22] The Copyright Act of 1957
[23] The Trade Marks Act of 1999.
[24] The Constitution of India.
[25] *Copyright* (n 22).
[26] ibid s.14. (The meanings of copyright under different categories are elaborated through this section. The categories range from literary work, musical work, dramatic work, artistic work, cinematographic film, sound recording).
[27] ibid.
[28] ibid s.51. (Works like sale or hire, distribution, execution in public, reproduction which amounts to infringement are elaborated through this section)

involve copying any copyrighted material, but synthetically generate audio-visual content using a person's face, voice, or gestures as with AI-created political speeches or celebrity pornography. In such cases, the deepfake creator bypasses the original copyrighted content and generates new material, leaving victims outside the protection of copyright laws unless the AI model itself infringes on a copyrighted dataset. Thus, while the Copyright Act offers useful provisions in specific contexts, it largely fails to address the core harm of deepfakes: the unauthorised appropriation of identity.[29]

Indian copyright law reaches out to the uniqueness of moral rights by section 57[30] where authors ask for authorship of their work and object to in case of distortion, mutilation, or other modification that harms their reputation. At the very stage of tarnished professional persona by manipulated deepfake this section comes as a knight. Likewise, a motivational speaker whose deepfake video to deliver profanes or misleading messages may claim for breach of moral rights, rowing that their reputation and honour have been compromised.[31] The limitation of Section 57[32] is that it applies only to authors of original works, not to ordinary individuals targeted by deepfakes for whom no authored content is involved. Therefore, while this section is helpful in selecting creative contexts, it is insufficient as a remedy for most deepfake victims.[33]

B. Trade Mark Law

While the Trade Marks Act[34] secures names, symbols, and marks that identify goods or services in commercial trading it has spread well in cases of celebrity endorsement and image rights. Section 29[35] highlight as deepfakes falsely attribute endorsements to public figures. In the event that a famous person has trademarked their name and brand, this provision might be invoked to cover a phoney video of a cricketer endorsing a bitcoin program.[36] In *ICC Development (International) Ltd. v. Arvee Enterprises*[37], the Delhi High Court ruled that right to publicity

[29] Ghosh S, 'IP Law and AI: Revisiting Indian Copyright in the Deepfake Era' (2020) 15 NALSAR Law Review 45
[30] *Copyright* (n 27).
[31] Bhatia G, 'Off the Hook: Why Indian Copyright Law Fails Deepfake Victims' (2022) 6 Indian Journal of Intellectual Property 77.
[32] *Copyright* (n 30).
[33] Kumar R and Verma N, 'Moral Rights in a Post-Human Creative Landscape: The Challenge of Deepfakes' (2023) 9 Indian Bar Journal 113.
[34] Trade Marks (n 23).
[35] ibid s 29.
[36] Singh M, 'Trade Marks and Digital Identity: Protecting Persona in India' (2022) 14(2) IP Law Review 56
[37] 2003VIIAD(DELHI)405.

forms a part of the right to privacy and can be used to prevent unauthorised use of personal attributes. Though Indian trademark rules circled by commercial misuse and not towards non-commercial sector it offers narrow protection with limited practical impact.

C. Constitutional Protections: From Privacy to Digital Identity

Right to privacy secures spot under article 21 of Indian constitution by *Puttaswamy* case[38] which expands the leeway of personal liberty to include informational autonomy, bodily integrity, and decisional privacy. When deepfake hunts informational autonomy lost in the hole. Though privacy rights empower a person to drive his personal data including facial features, voice, and expression to be collected, stored, and used yet when deepfake mimics a person's face or voice without consent, it directly violates this autonomy, rendering the manipulation constitutionally offensive.[39] Non-consensual circulation of explicit content or politically morphed videos can irreversibly damage the dignity of individuals, particularly women and public figures. Thus article 21 extends strongest remedial foundation with the motto that privacy is "the constitutional core of human dignity." By breaching the state boundaries, the Supreme Court has conquered the horizontal application of harm by private entity. It demands a constitutional interpretation of digital identity rights that may evolve to include duties on platforms and tech developers to prevent abuse. This global approach under the General Data Protection Regulation (GDPR)[40] in the European Union blesses individuals with the right to be forgotten, a concept that could aid victims of deepfake content in seeking takedown or deletion.[41]

The fertile constitutional ground under article 21 lacks cultivation of right to personality or image integrity. Digital and performative sense of identity demands digital likeness as an extension of the self, and its non-consensual use as adrift to fundamental dignity. Anchoring personality rights within the constitution, is rowing a shield that not only protects against surveillance and data breaches but also against AI-enabled impersonation-a modern threat to personhood itself. A starking asymmetry where harm is actual and growing but protections are

[38] AIR 2018 SC (SUPP) 1841.

[39] Bhandari V, 'Privacy and the Indian Constitution: A Commentary on the Puttaswamy Judgment' (2018) 10 Journal of Constitutional Law 23

[40] General Data Protection Regulation (GDPR) (An European Union regulation that sets guidelines for the collection and processing of personal data. The regulation was approved by the European Parliament in 2016 and went into effect in 2018. It aims to provide individuals with more control over their personal data).

[41] European Commission, 'Data Protection in the EU: Rights for Citizens' (2021) <https://ec.europa.eu/info/law/law-topic/data-protection_en> accessed 2 May 2025

scattered bridging the legal rift by hybrid legal framework is of utmost need for harmonising constitutional values with technological realities.[42]

III. The Interplay of IPR, Deepfake Exploitation, and Constitutional Protections

In India IPR in force that proposes most of protections often falls flat on face in addressing the deepfake harms. The pillars of IPR like copyright, trademark, patent etc. are exclusively serving the commercial stadiums but lacks severely the non-commercial platforms. Exclusive rights are given against unaccredited reproduction or adaptations of original creation to the real owner by the Copyright Act, 1957[43].The application of this is witnessed in morphed deepfakes over artistic works like videos, audio recordings, or performances. But the real question comes in to the forefront when the target is an individual. What about individual's likeness? Deepfakes find its path in that dark rifts where copyright protection cannot reach, where a person's voice, appearance is manipulated without consent. The Act of 1957 explores to shield the moral rights concerning an author's reputation, fundamental to the craftsmanship under section 57 but trembled in shadowing the individual's persona from deepfakes where their identity is distorted by something that have never done.[44] While the Act of 1999 is there to screen the commercial squandering of celebrity names and likeness of brands stemming perplexity in the market place. [45] Like the previously mentioned statutes this regulation also touches the commercial end lacking personal instances. Though public figures fine themselves under this protective shadow but in broader spectrum it is inadequate. India needs to offset this vent enabling traditional IPR regulations to whisk with tech rights to fight back deepfake exploitation particularly for non-commercial uses.

The constitution of India put notable implication apropos the privacy, dignity, and freedom of expression. The right to privacy has made the heart of the concern relating to an individual's control over their likeness and voice. In the landmark case Justice K.S. Puttaswamy v. Union of India, the Supreme Court recognized the right to privacy as a fundamental right, connecting it to the dignity and autonomy of the individual.[46] Individual's personal autonomy likely voice, facial recognition are made important aspect by this judgement. In this digital era the monstrous

[42] Narayan S, 'Deepfakes and the Copyright Conundrum: India's Legal Vacuum' (2021) 5(3) Tech Law Journal of India 88.
[43] *Copyright* (n 32).
[44] ibid s 57.
[45] Trade Marks (n 35).
[46] *Singh* (n 36).

deepfakes encroaches in the field of human rights by distorting person's identity against their consent resulting emotional, psychological and reputational harm. Though the fundamental right freedom of speech and expression is subject to reasonable restrictions to protect public order, morality and individual reputations but deepfakes poses striking ultimatum to this. Misrepresenting someone especially in political discourse or public figures, amounts to violation of right to privacy and disrupts democratic processes. Easy manipulation of people power by technology targets directly the centre of democracy. Leaving a person emotionally distressed and reputationally damaged, broken and shattered as towards dignity leads to eventual sacrifice of right to life and personal dignity protected under article 21.

Digital India demands personal security. It screams for rights preserving names, images, voices and likeness etc. Although with several interpretations given by Supreme Court in relation to celebrity rights, India being a developing third world country still lacks statutes arming individual's digital persona. The Delhi high court recognised the unauthorised commercial use of someone's persona as violation concerning celebrity identity in the case of *Titan Industries Ltd. v Ramkumar Jewellers*.[47] But it did not extend to the broader issue of non-commercial, non-consensual exploitation of personal images through technology such as deepfakes. The rocketing augmentation of tech fakes staged extreme need for legal protection to individual identity. Today identity manipulation can be done by the split of second. This demands personal identity protection in non-commercial regime. To answer this cry Indian jurisprudence must answer in affirmation by recognising them as an extension of the right to privacy under Article 21[48]. The law should define personality rights as the right to control one's digital image, likeness, and voice, even in the absence of commercial exploitation, to ensure that individuals are not left vulnerable to the harmful consequences of deepfake technology. In non-commercial regime the Indian IPR frameworks fails to reign in its totality. The existing policies like right to privacy, freedom of expression need further refinement to conquer technological identity manipulation. In this tech century man's persona, likeness can be shielded by personality recognising laws that compliment the already existing IPR mechanisms.

IV. Judicial Trends and Case Law Analysis

The historical approach by Indian judiciary towards the rights and privacy is done through a

[47] *Titan Industries Ltd. v. Ramkumar Jewellers* [2003] Delhi High Court.
[48] *Constitution* (n 21) art 19, 21.

constitutional lens, emphasising dignity, autonomy, and freedom of expression. But the legal answers to emerging digital threats like deepfake exploitation continues to be shattered and instinctive. India with infinite skill tackled a mass of cases like this but scope for limitation is still there when addressing contemporary technological harms.

a) Dr. Naresh Trehan v. John Doe & Ors.: Dr. Naresh Trehan approached the Delhi High Court after a deepfake video, falsely showing him endorsing dubious medical remedies, went viral online. The manipulated content posed not only reputational harm but also a serious public health risk, potentially misleading viewers into following unverified treatments. Recognising the gravity of the situation, the court issued a John Doe injunction, compelling online platforms such as YouTube, Instagram, and Facebook to promptly take down the video and disclose the identity of its creator within 36 hours. This judgement affirms judicial intervention in cases involving health misinformation amplified through deepfakes. This case marked climacteric flagging towards endangered public welfare. It also reinforced the accountability of intermediaries under India's digital governance frameworks.[49]

b) *National Stock Exchange of India Ltd. v. Meta Platforms, Inc. & Ors.*: When the higher officials of National Stock Exchange (NSE) start getting depicted falsely this case protests against the potential to mislead investors and destabilise financial markets and the NSE sought immediate judicial intervention. The Delhi High Court responded by invoking Rule 3(1)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, to direct the swift removal of the fabricated content. The ruling demonstrated the judiciary's growing recognition of the economic harms posed by AI-generated misinformation and its willingness to operationalise intermediary liability mechanisms.[50]

c) *Rajat Sharma v. Union of India*: Veteran journalist Rajat Sharma filed a public interest litigation highlighting the unchecked spread of deepfakes targeting political figures during the 2024 general elections demanding both institutional safeguards and establishment of a specialised regulatory body to fight the maluses of electric synthetic media. The court directed the Ministry of Electronics and Information Technology

[49] *Global Health Ltd and Anr v John Doe and Ors* [2025] CS(COMM) 6/2025 (Delhi HC).
[50] *National Stock Exchange of India Ltd v Meta Platforms Inc and Ors* [2024] Interim Application (L) No. 23560 of 2024 in Com IPR Suit (L) No. 23443 of 2024 (Bombay HC).

(MeitY) to evaluate the suggestions by enforcing constitutional utility but didn't issue urgent mandates. Finally constitutional litigation can act as a catalyst for policy-level reform in emerging technological domains. [51]

d) ***Anil Kapoor v. Various Defendants*****:** When Bollywood actor anil Kapoor's name, voice and catchphrases are misappropriated via deepfake offer for humorous parodies without his consent the actor approached the Delhi High Court. The court has acted promptly to secure his digital persona by issuing permanent injunction restraining further dissemination. This judgment expanded the contours of personality rights in India, presenting that even seemingly benign uses of a person's likeness may be injurious if done against authorisation.[52]

e) ***Neela Film Productions Pvt. Ltd. v. Taarakmehtakaooltahchashmah.com & Ors.*****:** The High Court of Delhi has taken legal action against websites and platforms that are distributing AI-generated deepfake content involving characters from the popular television series "Taarak Mehta Ka Ooltah Chashmah." The court issued an ex parte ad interim injunction, which prohibits the defendants from infringing on the show's copyright and trademark. This case highlights the court's proactive approach to protecting intellectual property rights against violations related to AI and the unauthorized use of widely recognized media content.[53]

f) ***Arijit Singh v. Codible Ventures LLP & Ors.*****:** The well-known singer Arijit Singh was involved in a legal case brought before the Bombay High Court against several businesses that used artificial intelligence to replicate his voice and likeness without permission. The court issued an ex parte order, prohibiting the defendants from commercializing voice or other personal attributes. Arijit Singh sued companies that profited from using artificial intelligence to imitate his voice. The court's proactive injunction prohibits the unlicensed use of Singh's likeness, voice, and other characteristics across all forms of media, including digital and AI-generated works. This landmark ruling sets a precedent for protecting artists' rights against impersonation by

[51] *Rajat Sharma v Union of India* [2021] W.P.(C) No. 80 of 2021 (SC).
[52] *Anil Kapoor v Simply Life India and Ors* [2023] CS(COMM) No. 645 of 2023 (Delhi HC).
[53] *Neela Film Productions Pvt Ltd v Taarakmehtakaooltahchashmah.com and Ors* [2024] CS(COMM) No. 456 of 2024 (Delhi HC).

AI.[54]

g) ***Asian News International (ANI) v. OpenAI*:** The Delhi High Court in a lawsuit where ANI claimed that OpenAI had used its copyrighted content without permission to train its AI models. This usage allegedly resulted in the creation of fake news articles where ANI asserts to have been misrepresented as their own. This case raises important questions about whether current legal frameworks can effectively address such issues in the digital age. It highlights the challenges of preventing the unauthorized use of proprietary material in AI training, showcasing the complexity at the intersection of data privacy, copyright law, and artificial intelligence. In a related matter, ANI had also sued the Wikimedia Foundation for defamation concerning Wikipedia articles. Initially, the Delhi High Court ordered the removal of specific content and mandated the identification of the editors involved. Later, the Supreme Court overturned these orders, underscoring the importance of free speech and cautioning against blanket takedown requests. This case emphasizes the delicate balance that must be maintained in the digital realm between protecting reputations and upholding free speech.[55]

In the 2024 Indian General Elections, manipulated speeches, revitalized politicians using technology, and altered regional linguistic footage received significant attention. Unfortunately, these issues are not explicitly addressed in existing regulations; only sections 465 and 469 of the Indian Penal Code (IPC)[56] are invoked. This raises the question: is it solely a matter of forgery and defamation? This question remains unanswered to this day. The Election Commission of India issued a statement condemning the exploitation of AI technologies during election campaigns.[57] This situation sparked extensive public discourse and highlighted the urgent need for election reform to address the threats posed by deepfake technology to democratic systems. In response to a petition from journalists and legal professionals, the Delhi High Court directed the central government to establish a multidisciplinary committee to address deepfakes legally. This committee should include representatives from the Ministry of Electronics and Information Technology (MeitY), law enforcement, academia, and civil society. The court also requested a comprehensive report

[54] *Arijit Singh v Codible Ventures LLP and Ors* [2024] Interim Application (L) No. 23560 of 2024 in Com IPR Suit (L) No. 23443 of 2024 (Bombay HC).
[55] *Asian News International v OpenAI* [2024] CS(COMM) No. 789 of 2024 (Delhi HC).
[56] Indian Penal Code, 1860 s.465, 469.
[57] McCarthy, J.T. (2023). *The Rights of Publicity and Privacy*, Westlaw Treatise.

within three months. This represents a proactive approach to judicial reform, aiming to combat the challenges posed by synthetic media. It marks a significant shift in Indian jurisprudence from sporadic court interventions to the necessity for a systematic regulatory framework for synthetic media.[58]

Nuanced threats posed by deepfakes handled ineptly as constitutional, intellectual and tort-based remedies lost the hunt against commercial impersonation. India in one hand suppressed the commercial evils but lost in the maze of non-commercial exploitations. Very well witnessed in the case of *Titan Industries Ltd. v. Ramkumar Jewellers* (2012),[59] where Delhi high court granted an injunction against misuse of celebrity images without authority but pornography, political satire or defamation involving non-celebrities left unanswered. This narrow interpretation leaves victims of personal harm especially women, activists, and minorities without a clear legal pathway for redress. The emphasis on commercial exploitation eclipses the broader psychological, social, and dignity-related consequences of deepfake abuses.

A. Constitutional Gaps

When the Supreme Court in *Puttaswamy* recognised privacy as a fundamental right,[60] the judgement offered a ray of hope that law would stand beside individuals in the most intimate corners of their lives. But for those facing harm in the present day, the hope feels out of reach. When facial expression is stolen by an algorithm, voice twisted into words never said, or likeness placed into contexts that violate dignity, the Constitution seems distant silent. The judgment gave the language to speak of privacy, but little in the way of tools to defend it in real time. When such a situation happens the mentally and physically a person is exposed to something he or she never consented to. Help provided is just a mess of rules that don't quite fit. The situation is even worse when the perpetrator isn't even identifiable, just a screen, a faux name, or no trace at all. The harm is not only caused by the act, but also till the time it lasts. Even the Constitution states that a person has the right to privacy, this promise is often arrives late, after the humiliation has set in, the harm has been done.

B. IPR Limitations

In India, intellectual property laws like copyright and trademark were created to protect

[58] ibid.
[59] *Titan* (n 46).
[60] *Puttaswamy* (n 16).

people's identities, especially when their name or likeness is used without permission for commercial gain. If someone's face ends up in an ad or an endorsement without their approval, these laws are meant to help. However, deepfakes don't always fit into this framework. Take a deepfake video with someone's face manipulated for political reasons or explicit content these kinds of issues usually don't trigger the protections of intellectual property laws unless there's some direct financial harm or unauthorized use of copyrighted material.[61] Even the moral rights[62] designed to protect an artist's reputation, don't help when someone's digital identity is altered maliciously, outside the creative realm. The laws simply weren't built to handle the new kind of harm. Thus, when people become victims of deepfakes, no clear legal recourse can protect their identity.

India's Constitution guarantees the right to privacy and dignity under Article 21,[63] which should give people the protection they need when it comes to digital threats like deepfakes. However, the reality is that these constitutional protections are difficult to enforce. Victims of deepfakes often have to rely on broad privacy laws under the Sections 66E and 67[64], which weren't designed with AI-generated content in mind. These laws can be inconsistent in their application,[65] and it's hard to get justice through them. What makes this even harder is that constitutional claims typically require proof that the state has failed to act or is somehow complicit, but in deepfake cases, the perpetrator is often anonymous or from outside the country. This leaves victims feeling stuck, unsure how to protect their dignity and identity when the law doesn't seem to be keeping up with the digital age.

Enterprises though have composed a protective cycle focusing personal autonomy and identity where the digital harms do not find home. It is evident that the trilogy of IPR constitution and cyber laws terribly fails apart in direct clash with electrical evils.

V. Comparative Study

A. **South Africa: Constitutional Recognition and Emerging Challenges**

The Constitution of the Republic of South Africa protects the right to privacy under Section

[61] R Gupta, 'Deepfakes, Identity and Indian Law: Mapping Legal Voids in a Digital Age' (2022) 9(1) Journal of Law and Technology 14.
[62] *Copyright* (n 43).
[63] *Constitution* (n 47).
[64] *Technology* (n 13) s.66E, 67.
[65] ibid.

14,[66] providing a strong foundation for data protection and preservation. The Protection of Personal Information Act (POPI Act),[67] implemented in 2021, regulates the processing of personal information which includes biometric data, and establishes the Information Regulator to ensure compliance while processing such data. According to POPI Act, personal data can only be processed with the explicit consent of the subject or under specified legal justifications, while imposing strict responsibilities on the data controllers. Despite these legal frameworks, South Africa lacks specific proper regulations addressing the threat of deepfakes. Existing legal remedies rely mostly on tort and criminal law, often insufficient for the complexities of digital identity violations. The rise of deepfakes jeopardizes identity rights and highlights the very need for a more effective legal strategy to address liability and provide suitable remedies. South Africa is developing a national digital identification system aimed at consolidating identities, improving security, and enhancing access to government services. This initiative represents a crucial step toward protecting citizens' identities.

B. Germany: Proactive Legislative Measures and Constitutional Protections

Germany is leading the way in the regulating digital identity and deepfakes through a robust approach that prioritizes constitutional protections alongwith comprehensive data safeguarding measures. The German Basic Law[68] firmly acknowledges the universal right to personality, encompassing both the right to one's appearance and voice. Under the BDSG[69] which operates in harmony with the GDPR[70] strict regulations govern data protection particularly concerning biometric data. It mandates that biometric data requires explicit consent, ensuring individuals retain rights to access their information, demand erasure, and pursue compensation in cases of misuse. In response to the profound threats posed by deepfakes, Germany's Federal Council has proactively introduced a draft law in July 2024 aimed at imposing serious penalties for the creation and dissemination of deepfakes that violate personal rights. This proposed legislation seeks to amend the German Criminal Code by adding Section 201b,[71] which provides for

[66] Constitution of Republic of South Africa 1996, s 14 (Everyone has the right to privacy which includes person, home or property not being searched, possession not seized and the privacy of communication not infringed).

[67] Protection Of Personal Information Act (POPI Act), 2023 (The preamble recognises section 14 of the Constitution of Republic of South Africa and states right to privacy includes protection against unlawful collection, retention, dissemination and using of personal information); The Promotion of Access to Information Act 2000.

[68] Basic Law for the Federal Republic of Germany (The Constitution of Federal Republic of Germany which came into effect on 23rd May 1949 which recognises under article 2 personal freedom).

[69] Federal Data Protection Act (BDSG) (A key piece of legislation that governs data protection and privacy and even sets up rules for how the personal data is to be collected, processed and stored).

[70] *GDPR* (n 40).

[71] DataGuidance, 'Germany: Bundesrat publishes draft law on deepfakes' (10 July 2024) <https :// www. data

significant penalties, including imprisonment and hefty fines. The unwavering commitment of Germany in strengthening its legal framework for escalating digital risks is highly impactful for the world at large.[72]

VI. Navigating the Legal Labyrinth

The absence of constitutional recognition for digital identity in India raises significant ethical and legal issues, especially as digital representations ranging from social media accounts to AI-generated deepfakes are now fundamental to both private and public life. The lack of cohesive safeguards and interpretive clarity stems from this gap in understanding how the Constitution, the IT Act, and intellectual property regulations interact with one another.

a) The Constitutional Landscape: Recognizing Privacy but Overlooking Digital Identity:

The Supreme Court's landmark decision in *Puttaswamy*[73] firmly established the right to privacy as a fundamental right under Article 21 of the Constitution. This ruling underscores the crucial importance of personal autonomy and informational privacy. However, it explicitly fails to address the concept of digital identity the unique digital representation of an individual that encompasses personal data, photographs, and online behaviors. This gap in the ruling introduces ambiguity into constitutional doctrine, leaving individuals' authority over their digital identities insufficiently defined. The Indian Constitution must recognize the right to digital identity. While the Supreme Court's affirmation of the right to privacy in the *Puttaswamy* case is significant, it does not extend to full control over one's digital identity. The absence of constitutional protection for digital identity rights compromises individuals' safeguards against the exploitation of their digital representations.

b) Information Technology Act, 2000: Addressing Cyber Offenses without a Digital Identity Framework:

The IT Act is India's primary law governing cyber-related offenses, specifically targeting identity theft and privacy violations under Sections 66C and 66E. However, these provisions

guidance.com/news/germany-bundesrat-publishes-draft-law-deepfakes> accessed 21 May 2025 (Section 201b is titled as "Violation of Personal Rights Through Digital Forgery,")

[72] Digital Policy Alert, 'Germany: Introduced Bill relating to criminal protection of personality rights against deepfakes' (5 July 2024) <https://digitalpolicyalert.org/event/21354-introduced-bill-relating-to-criminal-protection-of-personal-rights-against-deepfakes> accessed 21 May 2025.

[73] *Puttaswamy* (n 65).

are reactive and do not create a proactive framework. The law lacks comprehensive definitions and protections against issues like deepfakes, limiting legal options for victims.

Section 66C- addresses identity theft by penalizing unauthorized use of electronic signatures and unique identifiers.[74]

Section 66E- penalizes the unauthorized capture and distribution of private images, infringing the privacy rights.[75]

Despite these sections offering some legal remedies, they do not adequately cover the production or distribution of deepfakes, leaving victims vulnerable. The challenge is further compounded by the evolving use of biometric data, as highlighted by the Digital Personal Data Protection Act (DPDP Act).[76] While biometric data is crucial in various sectors, its collection raises significant privacy concerns. The interplay between the IT Act and the DPDP Act reveals inconsistencies in protecting digital identities. The IT Act addresses specific cyber crimes but lacks a comprehensive digital identity framework, while the DPDP Act offers protections that come with exemptions potentially undermining privacy rights. A cohesive legal strategy is needed to ensure effective protection of digital identities in India.

c) Intellectual Property Law: Protecting Economic Interests over Personal Identity:

India's intellectual property laws, comprising the Copyright Act and the Trade Marks Act, are fundamentally intended to safeguard the economic interests of creators and brand owners. However, these regulations are increasingly inadequate in addressing the non-commercial and harmful exploitation of digital identities, particularly in the context of deepfakes. A deepfake video that tarnishes an individual's reputation without any commercial intent often escapes the protective umbrella of current intellectual property rights, leaving victims without effective recourse. Furthermore, India's intellectual property system mostly stresses on the protection of commercial rights connected with creative works and brand identities, therefore overlooking the significant issue of illegal exploitation of personal traits in deepfakes. While a celebrity can seek trademark protection for the commercial exploitation of their likeness, an ordinary

[74] *Technolgy* (n 63) s.66C.
[75] ibid s.66E.
[76] The Digital Personal Data Protection Act, 2023. (The act is designed to protect individual's rights regarding their personal data, regulation of those personal data and ensuring that data is handles in a lawful and fair manner.)

individual finds themselves powerless against the damaging effects of non-consensual deepfake material. This gap in legal protection is not merely an oversight; but a critical vulnerability that undermines personal dignity and the integrity of individual identities in digital age. It is imperative to address these shortcomings while ensure justice and protection for all individuals, regardless of their status.[77]

VII. Conclusion

India's legal framework has a glaring deficiency; it lacks a legislative right to an individual's digital identity. While many jurisdictions safeguard personality rights, the present law fails to protect individuals from the unauthorized use of their likeness, voice, or other personal attributes in digital formats. In a world where AI can easily manipulate our images and voices the current system isn't equipped to protect people's digital identities. An advanced legal framework is required one that addresses both the commercial and personal harm caused by deepfakes. For the law to catch up with technology, the need of the hour is:

- Amendment or Interpretation to the Constitution: Digital identity must be recognized as a crucial element to the right to privacy and dignity under Article 21. Without this recognition establishing legal principles for protection would be insufficient.

- Amendment to the Criminal Laws: The definition of cyber crime must include making and sharing of deepfakes.

- Legislative Reforms: Emerging fraudulent activities like deepfakes needs to addressed through amendment in the IT Act.

- Enhancing Intellectual Property Law Protections: Legislation relating to IPR must be interpreted to include personal rights relating to voice and appearance regardless of commercial motives.

- Shaping the privacy laws: The laws relating to privacy at present day leads to murkiness. An individual's image to biometric needs to be encrypted, violation of which shall be penalised.

[77] Aharon Barak, *Human Dignity: The Constitutional Value and the Constitutional Right* (Cambridge University Press 2015).

- Judicial Engagement: The Court for protecting digital identities needs to actively step up and interpret the existing laws with the help of legal precedents and provide the justice to the victims.

Additionally the courts need to interpret existing laws in a way that recognizes the new challenges posed by AI technology. Robust regulations of AI platforms, along with better cyber policing are required to prevent harmful and unbridled content. As it says the sooner the better, delay in taking action will lead to significant harm. The digital era demands a revaluation of legal structures to protect individuals' rights in both phygital realms. In such an increasingly interconnected society laws relating to constitutional law, cyber laws and intellectual property laws needs to be connected and interpreted to uphold the privacy and dignity of individuals. The current legal system in India is not equipped to address advancing challenges like deepfakes. These challenges to be tackled requires a comprehensive strategy, including amendments to legislation, judicial recognition of digital identity rights, and public awareness campaigns. By enhancing the legal framework, India can more effectively protect individual rights in the advancing digital era and uphold the principles of privacy, dignity.