ARTICLE

DUAL-VICTIMISATION IN THE AGE OF AI-GENERATED DEEPFAKES: PERSONALITY RIGHTS VIOLATION & PUBLIC DECEPTION

Himanshi Jain*

Abstract

The sudden rise of deepfake technology, is one of the results of successful Artificial Intelligence (AI) transformation. Today, the deepfake technology has dual-use of showcasing creativity alongside fabricating media. While its initial use was confined to entertainment, its misuse in defamation, privacy violations, manipulation, and fraud has raised significant legal and societal challenges worldwide. The misinformation spreading across the social media platforms has created an urgent need for regulatory intervention and a focus on ethical standards. As tools to create deepfakes become more accessible, they are being used to harm people every day. The paper employs a case study approach to examine the modus operandi of deepfake scams and their associated financial, political, and societal harms. It reveals that such AI-generated content has the potential to undermine public trust in individuals and institutions. The findings indicate that although these deepfake scams do not cause direct physical harm, they influence decision-making, manipulate perceptions, and erode trust. The paper further introduces the concept of dual-victimisation, highlighting that perpetrators target celebrities for their likeness, and the general public becomes the ultimate victim through deception. Deepfake technology gives rise to various challenges including technological, psychological, societal, and legal. The paper applies a doctrinal approach along with content analysis to examine judicial pronouncements and the legal positioning of AI-driven deepfake scams. The findings reveal multiple factors that facilitate the successful execution of the fraud, such as consumer awareness, institutional safeguards, and Indian legal frameworks. The paper concludes with recommendations to promote AI governance, enhance detection mechanisms, and increase international cooperation to expand protection in digital environments.

Keywords – Artificial Intelligence (AI), Deepfake Scams, Cyber Fraud, Digital Transformation, Personality Rights

I. THE ADVENT OF SYNTHETIC MEDIA: AI-GENERATED DEEPFAKES

There is a commendable transformation in the field of technology that is reshaping communication, creativity, and information exchange which has simultaneously led to the emergence of unprecedented challenges in the digital landscape. Advances in AI have enabled the creation of content in highly realistic forms in digital media. Although it fosters creativity and innovation, AI-generated content on various social media websites is altering traditional patterns of how social media used to function. Among these innovations, Deepfake technology

* PhD Scholar, Dr. Ram Manohar Lohiya National Law University, Lucknow, Uttar Pradesh.

is one of the most controversial developments in a long history of technological manifestations that has dual-use nature of serving creativity and harmful applications. These technologies were developed with an intent to are meant to benefit the society; however, they have now become tools of exploitation, extortion, and defamation. Whether this transformation is a boon or a bane remains a matter of debate; on the one hand, it serves as a tool to showcase one's innovation, while on the other hand, it facilitates the spread of misinformation.

There is a process for training machine learning models using deep learning techniques, generative adversarial networks, AI Algorithms, and advanced processing methods to create highly realistic audio-video content.[82] The synthetic media is generated by feeding large datasets, such as images, audios and videos of a specific person to machine learning models.[83] As a result, these models learn to imitate the target's facial expressions, voice modulation, and mannerisms with striking accuracy making it difficult to distinguish from authentic content. By applying these technologies together, it becomes able to produce false representations, depict individuals in situations, and generate evidence of events that never occurred. It is concerning to come across AI-generated content that presents fabricated depictions of real people, places, and events. This technology has been used to replicate an individual's voice in fraudulent scams, such as voice cloning, thereby demonstrating the potential misuse of generative AI.

By the year 2017, deepfake technology was widely available across the digital landscape. While its earlier usage was confined to entertainment and parody, creators posed celebrities in humorous videos. However, this initial phase did not last long, and deepfakes took a troubling turn. By the year 2020, perpetrators were actively using deepfakes for harmful purposes, such as the creation of non-consensual explicit content, fraud, harassment, and political manipulation. Earlier, the term "*deepfake*" was used to refer to the face-swapping videos that were made using deep neural networks; however, in today's time, the word "*deepfake*" encompasses a sophisticated ecosystem of manipulation.

The widespread use of social networking sites among youth heightens this risk, as they frequently consume digital content and often lack the digital literacy needed to identify manipulated content.

It is rightly observed that deepfakes can give rise to "*liar's dividend*", in which genuine information can be discarded by claiming it is fake.[84] The increasing misuse of celebrity identities in scams highlights a dual-layered harm arrangement. On one hand, perpetrators use celebrities to manipulate the general public, while celebrities themselves become victims of unauthorized exploitation. On the other hand, the general public is duped by false representations, thereby referring to it as dual victimization. It violates celebrities' personality (publicity) rights, harms their reputations, amplifies distrust in institutions, and misleads the public into making decisions based on false representations. The two significant factors that lead to the successful implementation of these scams are: the highly realistic nature of the content that blurs the line between authenticity and fabrication, the other one is the strong and emotional psychological connection between the general public and celebrities making it difficult to know

---

[82] A.K. Roundtree, *Deepfake Laws Protecting Childhood Safety and Future: An NLP Analysis*, Interaction Design and Children (IDC '25) 1086, 1086–1090 (2025), https://doi.org/10.1145/3713043.3731535.

[83] John Twomey et al., *"What Do You Expect? You're Part of the Internet": Analyzing Celebrities' Experiences as Usees of Deepfake Technology* (2025), https://doi.org/10.48550/arXiv.2507.13065.

[84] *Increasing Threats of Deepfake Identities*, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.

what to trust and what not to. This emotional reliance, sense of excitement, and urgency override one's cognitive understanding, leading one to fall prey to manipulation.

II. DEEPFAKE HARMS IN PRACTICE: FINANCIAL, POLITICAL, SOCIAL

When trust turns costly:

The growing incidents of deepfake technology scams follow a clear pattern of misusing the credibility of well-known personalities to manipulate and deceive the general public. Scammers employ high-quality AI tools to generate realistic audio and video content that imitates prominent global and Indian celebrities. The modus operandi of the perpetrators operates by convincing the public about various schemes, including fake giveaways, cryptocurrency schemes, fabricated endorsements, and fraudulent investment platforms.

It has been evident in multiple cases, such as a woman residing in South Los Angeles who was defrauded of thousands of dollars via an AI-generated scam featuring Steve Burton.[85] Another scam took place in India, where deepfake videos featuring National Stock Exchange (NSE)'s CEO Ashish Kumar Chauhan were found on the internet offering stock recommendations, prompting the NSE to issue a public warning.[86] Furthermore, even the judiciary has recognized this issue where the Delhi High Court addressed the misuse of the veteran actor Amitabh Bachchan's personality rights in KBC lottery scams circulating on WhatsApp.[87]

The abovementioned incidents show a fundamental shift in the ways digital frauds are operating and illustrate how readily available AI tools can replicate an individual's characteristics with minimal data. These are clear examples of perpetrators not just hacking systems anymore, but exploiting human trust.

Manipulating public opinions

Deepfake technology is used to manipulate politics, especially during election periods. Recently, Kerala police registered a case where an AI-generated video was circulated on X (Twitter) depicting Prime Minister Narendra Modi and Chief Election Commissioner (CEC) Gyanesh Kumar.[88] As the elections approach, such content has the potential to mislead voters and cast doubt on the election's fairness. In another instance, a deepfake video showing Manoj Tiwari criticizing the opposition was disseminated through WhatsApp.[89] State police departments

---

[85] Kevin Ozebek, *"General Hospital" Actor Steve Burton Deepfake Scam: Experts Break Down Top Ways to Spot a Fake AI Video*, ABC7 Chicago (Aug. 28, 2025), https://abc7chicago.com/post/general-hospital-actor-steve-burton-deepfake-scam-experts-break-down-top-ways-spot-fake-ai-video/17665484/.

[86] *Beware of Deepfake CEO Recommending Stocks, Says India's National Stock Exchange*, Reuters (Apr. 11, 2024), https://www.reuters.com/technology/cybersecurity/beware-deepfake-ceo-recommending-stocks-says-indias-national-stock-exchange-2024-04-10/.

[87] PTI, *Unauthorised Use of Amitabh Bachchan's Voice, Image Barred by Delhi HC*, Financial Express (Nov. 25, 2022), https://www.financialexpress.com/india-news/unauthorised-use-of-amitabh-bachchans-voice-image-barred-by-delhi-hc/2891988/.

[88] Shaju Philip, *Row over EC Letter with BJP Seal: AI Video of PM, Chief Election Commissioner Leads to Kerala Police Case*, Indian Express (Mar. 26, 2026), https://indianexpress.com/article/india/row-letter-bjp-seal-ai-video-of-pm-chief-election-commissioner-kerala-10602240/.

[89] John Xavier, *Deepfakes Enter Indian Election Campaigns*, The Hindu (Apr. 16, 2024), https://www.thehindu.com/news/national/deepfakes-enter-indian-election-campaigns/article61628550.ece.

occasionally register criminal cases involving AI-generated content that are detected, while many more cases remain undetected. There are far more that go undetected.

The political deepfakes operate differently from financial deepfake scams, as the primary impact lies not in financial loss but in a more insidious threat: the manipulation of public opinion. They have the capacity to influence voter behavior and undermine electoral fairness, which is the foundation of free and fair elections and democratic governance.

Amplifiers of threat and social tensions

A notable instance of how a deepfake video can induce social instability. In 2022, a fabricated AI video of Volodymyr Zelenskyy appeared online, showing him urging citizens to surrender to Russia. The video showed up strategically during the Ukraine-Russia war, although the Ukrainian government had already warned its citizens about such tactics used by Russia as part of information warfare.[90] This case clearly illustrates how perpetrators use synthetic media to spread misleading narratives and disrupt public confidence during such critical moments.

Upon employing a case study-based approach, it can be stated that there is a consistent pattern of not merely deceiving but also exploiting public trust at large. The fact that well-educated people fell prey to these scams suggests a high level of vulnerability among the uneducated population in less developed regions. As individuals with limited education are also active digital users, scammers can now easily obtain personal information. From the fabricated narratives to the neatly staged setups can escalate coercion, panic, and anxiety in victims.

Most importantly, these instances reveal that the consequences of deepfake scams are not confined to a single individual but rather operate on a dual-layered harm arrangement. It is to say that the first victim of such an arrangement is the one whose identity is misused, and the second victim is the audience, who is deceived; therefore, the injuries are interconnected. It showcases the concept of dual-victimization in the context of deepfake misuse.

III. UNDERSTANDING DUAL-VICTIMISATION: IDENTITY EXPLOITATION AND PUBLIC DECEPTION

Celebrities as primary victims:

Deepfake technology has a dual nature, combining the potential to showcase one's creativity with the potential for deception, manipulation, and privacy violations. Deepfakes are not only technical artifacts but also powerful communication tools capable of reshaping one's perception. Today, it is not only operating as a medium for spreading information in the domains of advertising and entertainment, but also simultaneously eroding trust and reputation. Upon examining deepfake scam cases, it is revealed that celebrities' likenesses are often used as a tool to establish credibility and bridge the trust gap between scammers and the general public. In the context of celebrity, it includes Bollywood actors, content creators, politicians, and other well-known personalities. They are becoming the targets through the misuse of their likeness for misinformation, which facilitates successful deception. Often, they remain unaware of such

[90] Tom Simonite, *A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be*, WIRED (Mar. 17, 2022), https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.

creations, leading to a violation of their consent and autonomy, this is referred as "Usees". The word "*Usees*" refers to unaware individuals who did not consent and became the direct targets of technology.[91] Deepfake technology targets them first

This highlights an inherent power dynamic deeply engraved in current legal frameworks, which gives greater protection to platform and website creators than to the victims. As the celebrities are the first targets of the deepfake scams, they bear a responsibility to advocate for legal and regulatory changes. The online presence of the celebrities is often justified by the abuse they face, normalizing the idea that harassment is a part and parcel of internet culture. There is a clear irony in how social media can facilitate deepfake harm while also becoming a primary means through which victims become aware of such violations.

General public as ultimate victims:

The analysis of these instances reveals a pattern in which celebrities are the direct targets of deepfake scams, while the broader public is the indirect yet ultimate targets.[92] Perpetrators misuse a celebrity's attributes to gain trust and create an emotional connection with the ultimate target. People tend to associate celebrities with credibility, which reduces public scepticism. Psychologically, if a familiar face appears endorsing a product, investment scheme, or message, people are likely to believe it on face value without verifying it with credible sources. People often admire and look up to these personalities which fosters excitement and a sense of urgency when such offers and opportunities are presented before them. Amid these emotions, cognitive thinking takes a back seat, leaving them more vulnerable to such scams. In this way, deepfakes turn public trust into a tool of deception.

The arrangement leads to *dual-victimisation*, wherein celebrities face violations of their personality rights and privacy, and damage to their reputations, while the general public face financial and psychological losses. This prompts a critical question: who experiences the greater degree of harm?

IV. THE CHALLENGES ASSOCIATED WITH AI-GENERATED DEEPFAKES

Platform Failures:

There is a significant gap in the existing literature on deepfake technology; it often fails to examine the role of digital platforms in facilitating the spread of such content. A disproportionate burden is placed on the victims to detect, report, and seek its removal.[93] These self-reporting mechanisms are problematic because victims are unaware of the existence of such content. While search engines and internet service providers have the technical capacity to detect and take down such content, they do not take any proactive measures. Additionally, platform governance is inadequate, and the harmful AI-generated content bypasses scrutiny. Although reporting mechanisms exist on each social media platform, there is a noticeable delay in platform

[91] E.P.S. Baumer, *Usees*, in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)* 3295, 3295–3298 (2015), https://doi.org/10.1145/2702123.2702147.

[92] B. Timmerman et al., *Studying the Online Deepfake Community*, 2 J. Online Trust & Safety (2023), https://tsjournal.org/index.php/jots/article/view/126.

[93] P.N. Vasist & S. Krishnan, *Engaging with Deepfakes: A Meta-Synthesis from the Perspective of Social Shaping of Technology Theory*, 33 Internet Research 1670, 1670–1726 (2023), https://doi.org/10.1108/INTR-06-2022-0465.

responses, and complaints are not addressed in a timely manner, reducing the effectiveness of these remedial measures. Some platforms have taken active steps, such as AI detection tools and labelling for AI-generated content.

Today, some open-source deepfake technologies are associated with platforms that produce *non-consensual intimate imagery (NSII)*.[94] Many of these tools are equipped with pre-trained models based on real individuals.[95] The developers of these technologies often position themselves as neutral and absolve themselves of responsibility, while in reality, these tools enable and encourage exploitative practices.

Technological Complexities:

The technical complexity is increasing manifoldly. Deep learning algorithms, advanced computer vision systems, and *generative adversarial networks (GANs)* pose a major challenge for existing legal systems.[96] It often exceeds judges' technical literacy, posing a significant challenge for assessing deepfake content as evidence. Many deepfake technologies disregard the importance of obtaining consent from the individuals depicted in them. It is found that the existing detection tools are not entirely reliable; they produce false positives and false negatives, which creates evidentiary uncertainty.[97] There is continuous evolution in deepfake technology; however, detection tools cannot keep pace and become obsolete over time.

Psychological Vulnerabilities:

Beyond technological concerns, deepfakes pose significant psychological challenges for the audience. The first impression is deeply ingrained in cognitive memory and is particularly difficult to reverse.[98] This is called "*illusory truth effect*" which describes the tendency of individuals who are once exposed to fabricated content to continue to believe it despite subsequent official clarification.

Social Consequences

Social responses to deepfake harms often pressure victims to withdraw from digital spaces, thereby encouraging perpetrators and diverting attention from the root cause of the harm.[99] These calls for urgent enhanced digital literacy can serve as a key mechanism to combat manipulation. Owing to growing awareness, many users attempt to evaluate credibility through various methods; however, these efforts fail against highly realistic AI-generated content. This creates a

---

[94] Saddam Hossain et al., *Social and Psychological Impact of Deepfakes: A Comprehensive Bibliometric Review*, Global Knowledge, Memory & Communication 1, 1–20 (2024), https://doi.org/10.1108/GKMC-11-2024-0734.

[95] A. McCosker, *Making Sense of Deepfakes: Socializing AI and Building Data Literacy on GitHub and YouTube*, 26 New Media & Society 2786, 2786–2803 (2024), https://www.scirp.org/reference/referencespapers?referenceid=4000211.

[96] Goodfellow, et al., *Generative adversarial nets*, 27 Advances in Neural Information Processing Systems 2672, 2672-2680 (2014), http://papers.neurips.cc/paper/5423-generative-adversarial-nets.pdf.

[97] L. Whittaker et al., *Mapping the Deepfake Landscape for Innovation: A Multidisciplinary Systematic Review and Future Research Agenda*, 125 Technovation 102784 (2023), https://www.researchgate.net/publication/370984566_Mapping_the_deepfake_landscape_for_innovation_A_multidisciplinary_systematic_review_and_future_research_agenda.

[98] A. Kukreti et al., *The Impact of Deepfake Technology on Legal Systems: A Global Perspective*, 7 ShodhKosh: J. Visual & Performing Arts 530, 530–544 (2026), https://doi.org/10.29121/shodhkosh.v7.i1s.2026.7068.

[99] Furizal et al., *Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review*, 12 Soc. Sci. & Human. Open 101882, (2025), https://doi.org/10.1016/J.SSAHO.2025.101882.

dangerous environment for users, especially youth who struggle to distinguish between truth and tech, thereby manipulating their decision-making capabilities.

Legal Limitations:

The Indian legal frameworks were developed in the pre-digital era, which makes them ill-equipped to manage the pace of growing deepfake technologies. Even with amendments and new laws, deepfake technologies continue to evolve, creating new vulnerabilities. Another significant problem lies in cross-border enforcement and the absence of global cooperation treaties hinder effective prosecution. The perpetrators exploit jurisdictional gaps and diverse legal systems, leaving victims with fragmented avenues to seek redress.[100] The deepfakes cycle involves multiple actors: the person who created it, the person who modified it, the person who distributed it, and, lastly, everyone who shared it. Therefore, establishing the appropriate defendant in legal proceedings further complicates the situation.

The conventional legal categories, such as defamation, copyright, and personality rights exploitation, and privacy infringement, remain insufficient for addressing deepfakes across the full spectrum. The laws were created to protect one from commercial exploitation, but they fall short in non-commercial exploitation, such as harassment, revenge, and political manipulation.[101] Another challenge is proving the authenticity of digital content, which creates evidentiary uncertainty. Moreover, the viral nature of online content's spread across social media further diminishes the effectiveness of legal remedies. The content is often widely circulated long before any corrective legal action can be taken.

V. STATUTORY PROVISIONS AND JUDICIAL RESPONSES TO AI-GENERATED DEEPFAKES

The Information Technology Act (IT Act), 2000, serves as the foundation of India's cyber law system. As of now, there is no specific offence defined that addresses the offence of committing scams using deepfakes of famous personalities. In the absence of specific legislation on deepfakes, the existing provisions that can be invoked as per the IT Act are *identity fraud committed through electronic means*.[102] It can be applied to cases where deepfakes are used for identity fraud and impersonation. Another provision that can be invoked is the *publication or transmission of obscene material in electronic form*.[103] It can be applied in cases involving deepfake pornography.

Under the Bharatiya Nyaya Sanhita (BNS), 2023, several provisions may be invoked to regulate deepfake harms, those are as follows: *cheating by personation*[104], *penalizing for publishing and*

[100] Iqbal J, *Cybercrime in India: Trends and Challenges*, 6 International Journal of Innovations & Advancement in Computer Science 187, (2017), https://www.researchgate.net/publication/322245372_Cybercrime_in_India_Trends_and_Challenges.

[101] S. Aggarwal & D. Tripathi, *AI-Generated Content on Social Networking Sites: Reviewing Trust and Authenticity of the Users*, IEEE DELCON 1, 1–5 (2025), https://doi.org/10.1109/DELCON68055.2025.11400455.

[102] Information Technology Act (IT Act), 2000, § 66D, No. 21, Acts of Parliament, 2000 (India)

[103] Information Technology Act (IT Act), 2000, § 67, No. 21, Acts of Parliament, 2000 (India)

[104] Bharatiya Nyaya Sanhita (BNS), 2023, § 319, No. 45, Acts of Parliament, 2023 (India)

circulating false information to cause public mischief[105], *defamation*[106], *forgery*[107], and *organised crimes*[108] where deepfakes are systematically used to carry out large-scale cyber scams, these provisions are too broad and were not designed to address synthetic media in the first place; as a result, their application highlights a major gap in the Indian legal framework.

The Digital Personal Data Protection Act (DPDP)[109] primarily strengthen data protection, its application in the context of deepfake harms remains indirect and insufficient. The provisions in the Act do not directly protect one from the creation and dissemination of deepfakes, thereby highlighting a significant gap in addressing synthetic media.

These legal frameworks are inadequate when it comes to election-related misinformation spread, as they were primarily designed to address fraud and obscenity. Another major challenge to prosecuting such offences is their nature. These offences extend beyond jurisdictional boundaries, with perpetrators and victims located at far-flung corners of the world. Investigations into such cyber scams often result in a dead end due to inadequate cross-border cooperation. Delays in timely information sharing and in mutual legal assistance result in case closure without prosecution. Once a deepfake is created, it can rapidly spread and be replicated across jurisdictions by numerous individuals. They contribute to the spread rather than to creation, rendering the traditional legal liabilities inadequate. Similarly, the social media platforms also contribute to the widespread dissemination, and holding them accountable is legally impossible. The perpetrators are well aware of these limitations and will continue to exploit them until they have access to open-source technologies.

The Delhi High Court, in one of its rulings, extended the scope of personality rights to address digital likeness and AI-generated fabricated content. The Court recognized that AI technologies enable the creation of deepfake content and take control over one's digital identity. The Court issued an injunction in favour of the plaintiff, demonstrating judicial innovation in the absence of specific deepfake legislation.[110] Enforcing injunctions against numerous unknown individuals remains a practical challenge in such cases; therefore, this case illustrates the need for a legislative framework and social media platform policies.

Over the past few years, a growing number of prominent personalities have moved to the Delhi High Court to seek protection of their personality rights, particularly against emerging digital misuse. In 2025, nearly 25 well-known personalities across diverse fields, including news anchors, content creators, film actors, and spiritual leaders, approached the Delhi High Court to protect their personality rights.[111] This trend has brought the Court into the spotlight for all the right reasons. Therefore, the Delhi High Court became the primary venue for personality rights disputes.

With the rise of technology, courts are often asked how the traditional personality rights doctrine applies to AI-generated deepfake content. The Court held that a personality rights claim depends

[105] Bharatiya Nyaya Sanhita (BNS), 2023, § 353, No. 45, Acts of Parliament, 2023 (India)
[106] Bharatiya Nyaya Sanhita (BNS), 2023, § 356, No. 45, Acts of Parliament, 2023 (India)
[107] Bharatiya Nyaya Sanhita (BNS), 2023, § 336, No. 45, Acts of Parliament, 2023 (India)
[108] Bharatiya Nyaya Sanhita (BNS), 2023, § 111, No. 45, Acts of Parliament, 2023 (India)
[109] Digital Personal Data Protection Act (DPDPA), 2023, No. 22, Acts of Parliament, 2023 (India)
[110] Sadhguru Jagadish Vasudev v. Igor Isakov, (2025) SCC OnLine Del 3804
[111] LiveLaw News Network, *Personality Rights: All India Annual Digest 2025*, LiveLaw (Feb. 2, 2026), https://www.livelaw.in/high-court/all-india-annual-digest-2025-personality-rights-521370.

on the recognizability of the individual and the likelihood of consumer confusion regarding the endorsement. However, this framework may not apply to deepfakes in its entirety, as it is designed to look hyper-realistic. The Court protected free speech and expression in a video game containing creative, fictional elements, even though some aspects are similar to *Lohan's* appearance.[112]

This showcases different approaches to understanding personality rights in the context of AI-generated content. While the first approach protects from technological manipulation, the other one favours artistic freedom and expression.

VI. CONCLUSION AND SUGGESTIONS

The exponential growth of Artificial Intelligence (AI) has reshaped how information is created, shared, and consumed. Although, the internet is a medium of innovation and collaboration, alongside these advantages, there is a simultaneous growth in criminal activity as well. Deepfake technology is the product of AI innovation, introducing new dimensions of deception. The hyper-realistic synthetic media is created with minimal effort, which blurs the boundaries between real and artificial content. The technical innovation in AI, continues to outpace the ethical and legal policies, creating an urgent need for proactive intervention. As it has been found that the harms associated with deepfake scams are not directly physical, however, this should not negate their seriousness.

Through this paper the introduction of *dual-victimisation* highlights how harm is inflicted simultaneously at multiple levels. While public figures across various domains are often the visible victims, the general public ultimately bears the burden of deception. This makes them equally important subjects of legal and policy protection. The Indian legal frameworks in this context are fragmented and struggling to keep pace with technological developments.

This paper suggests that the best way to foster trust and transparency through AI and social media platforms can be done only by clearly labelling AI-generated content with watermarks, disclaimers. Additionally, they must take youth protection seriously, incorporating age verification systems. As digital technologies are deeply embedded in our daily lives, it is important to continuously strengthen public digital literacy, especially among youth, to address regarding emerging forms of public deception. The study further proposes to employ active public awareness strategies that can neutralise such scams at the first point of contact itself. The strategies shall not only focus on the risks of deepfakes but also on available policies, remedies and support systems for victims. The prior case studies have shown that AI-generated deepfakes are often created without the consent of the individuals depicted. Therefore, it is important to pay attention to both policy and practice. The Indian legal system must impose stricter penalties, proper implementation and acknowledge non-physical harms for both celebrities and the general public. Lastly, promoting ethical AI governance, technological accountability, and international collaborations can ensure dignity and trust in the digital environment.

[112] Lohan v. Take-Two Interactive Software, Inc., 73 N.Y.S.3d 780 (N.Y. 2018)