

Deepfakes as a form of Image-Based Sexual Abuse: An Analysis

Vivek. V. G¹ & Kavitha Balakrishnan²

Abstract

The advancement in Information and Communication facilities have made drastic changes in human life especially in the way of people communicate. However, these developments also have a darker side, giving rise to serious challenges through various forms online abuses. Among them, the introduction of Artificial Intelligence (AI) and creation of deepfakes images or videos are most concerning issue which demand high social and legal attention. This paper outlines legal and social issues in related to deepfakes and provided with suggestive legal solutions.

Keywords: Artificial intelligence- deepfakes- online abuses- image based sexual abuses

Introduction

The advent of Information and Communication Technologies (ICTs) has revolutionized how people communicate and access information making both simple and faster. However, this technological advent has also some devastating troubles and problems in digital space. It paved way for online abuses, among the most concerning developments is, the creation and widespread dissemination of fake sexualized images, often generated using artificial intelligence or deepfake technology. These manipulated images are typically produced without the consent of the individuals depicted and are circulated for purposes such as financial exploitation, targeted harassment, or sexual gratification. The simplicity of technology to make and disseminate such content has now amplified the psychological and reputational harm experienced by victims, while also challenging existing legal frameworks that struggle to keep pace with technological change. As these practices become more sophisticated and accessible, addressing them requires a combination of legal reform, technological safeguards, and public education.

What is meant by Image-Based Sexual Abuses?

Deepfakes is vicious form of Image-Based Sexual Abuse (hereinafter referred to as IBSA), posing a current, severe, and rapidly escalating threat. The IBSA can be described as the non-consensual making and circulating of sexually explicit images or videos. The concept of IBSA has been developed by Clare McGlynn and Erika Rackley which includes i) a person is coerced or intimidated into sending sexual communications; ii) intimate photographs are shared without consent; and iii) cyberflashing occurs when a person shows an image of their own genitalia to an

¹ Research Scholar, Department of Law, School of Legal Studies, Dr. Janaki Ammal Campus, Palayad.

² Assistant Professor, Department of Law, School of Legal Studies, Dr. Janaki Ammal Campus, Palayad.

unwary individual.(Sparks et al., 2023, p. 2) As the part of pornography, it is not a newly identified class of offences in the world. In various forms and on various platforms, non-consented pornographic contents were present in the past. Pornography can be traced back to dawn of civilization and had existed in the form of paintings. The pornography was existed in almost all societies including the traditional societies like ancient Babylon, ancient Hindu society etc., Thus the existence of pornography is centuries old. But the revolution in the area of information and communication technology in 21st century provided a freely and speedy accessible platform for spreading of pornography and more especially the IBSA. The globalization of communication is essential for human being, but at the same time it also paved way for globalization of IBSA. The IBSA is a cybercrime in the form of cyber bullying, sexting, revenge porn, cyber flashing etc., Mostly women are being subjected to this kind of cyber atrocities. Internet have been uses as a potential tool for threatening and harassing women. Men have also been subjected to IBSA by the way of honey trap or blackmailing. The IBSA are mushrooming worldwide into an alarming situation, where the attention of law-making bodies, law implementing agencies, psychologist, media needed.

Deepfakes as a form of IBSA

Deepfakes involve the non-consensual creation and dissemination of sexually explicit images or videos using widely accessible artificial intelligence tools. These manipulations are often so realistic that they create an indistinguishable illusion, leading viewers to believe that the targeted individual is genuinely engaging in a sexual act. This technology enables perpetrators to inflict significant psychological harm, reputational damage, and emotional distress on victims, often without any physical contact or direct interaction. As such, deepfakes represent a particularly insidious form of IBSA, exploiting technological advancement to violate privacy and consent on an unprecedented scale.(Fido et al., 2022, p. 1) Deepfakes are synthetic media generated by artificially intelligent techniques that alter a person's appearance in audio, video, or image formats. The *Oxford Advanced Learner's Dictionary* defines "deepfake" as a noun, referring to a video where a person's appearance has been digitally altered to make them look like someone else.(*Oxford Learner's Dictionaries*, n.d.)The EU AI Act also defines deepfakes as AI-generated or manipulated content that mimics real persons or events, potentially deceiving viewers into believing it is authentic (Article 3(60)). Various techniques are used to create deepfakes, but at their core, they employ AI to replicate or alter object's appearances. Not all deepfakes are evil, notwithstanding the fact that they are frequently associated with bad applications. They may have educational applications, such as individualized training resources that improve learning results. Deepfakes can also be used for cultural purposes. For example, the Salvador Dali deepfake that welcomes guests to the Dali Museum in Florida increases interest in the artist's creations. But according to De Ruiter, the unethical use of deepfakes happens when digital representations are made

without agreement, especially when they show people in ways they wouldn't want to be seen.(Kira, 2024, p. 2)

Together, offenses including upskirting, revenge pornography, and cyber-flashing constitute the wider umbrella of IBSA, of which deepfakes have grown into a particularly complex and harmful subcategory. Video, audio, and various other types of content that are either entirely or partially fake, or pre-existing images or videos that has been digitally modified or altered, are referred to as deepfakes. In addition to changing the pitch, timbre, and even the language of audio content, contemporary deepfake technology allows for the frame-by-frame manipulation of facial expressions. Additionally, it can combine the identities of several people, for example, by overlaying one person's face on another's body or fusing one person's voice with another's looks. These adjustments can produce incredibly realistic simulations that trick viewers into thinking the material is real, thus thereby amplifying the harm to the targeted individuals.(van der Sloot & Wagenveld, 2022, p. 1).

Deepfake technology uses advanced artificial intelligence techniques, especially neural networks and Generative Adversarial Networks (GANs), to change existing content in a way that represents someone or something else. Although these technologies have valid uses, they can easily be misused in a variety of situations. Deepfake systems may realistically change a person's speech, facial expressions, and environment, which frequently gives the faked material an incredibly realistic appearance. The likelihood of dishonesty is greatly increased by this realism. People and society as a whole are seriously threatened by the malicious creation and distribution of such modified content, particularly when it is used for impersonation or the spread of misleading information. In addition to creating difficult moral and legal issues, it can weaken public faith in digital media, harm reputations, and undermine trust.(Wazid et al., 2024, p. 1)

Deepfake productions target female celebrities disproportionately because of their high public visibility and extensive online presence. Since their photos and videos are easily accessible on a variety of media platforms, AI tools could be used to manipulate them. These deepfakes, which are frequently sexual in nature and shared without permission, are part of a type of online gender-based violence that takes advantage of both gender and celebrity. This targeting is a reflection of larger cultural trends of objectification and misogyny, in which women's bodies are weaponized and commodified for amusement, harassment, or financial gain.(Fido et al., 2022, p. 1) Because such behaviours are inherent to being famous, female celebrities are increasingly becoming the focus of trolls and online abuses, including deep faking, as a result of antisocial behavior and hatred mediated by the internet.(Fido et al., 2022, p. 2) The perpetrators might be felt safer for their pervasive actions compare to non-celebrities due to social positions is distant from that of the ordinary peoples.

People who take sexual photos of themselves are sometimes labelled as reckless, careless, or naive, which implies that they should be well aware of the risks involved. This viewpoint holds that the image-taker is ultimately responsible for handling such photographs, including safely deleting them, especially after a relationship ends. This perspective frequently ignores the importance of agreement, trust, and the responsibility of people who decide to use such photographs for commercial purposes. It also assumes a high degree of foresight and control over personal digital property.(McGlynn et al., 2017)

Consequences of Deepfake Generations

Disclosing private sexual photographs with intent to cause distress to the victim is a high-profile internet-based problem where victim ashamed, hurt, violated, even broken at many times. In almost all cases of IBSA, sex may be consensual, but recording of videos or taking photos are not consensual. The peculiar feature of ibsa is that, on internet, once an information is posted, it is out there forever by redistribution, downloading, sharing and spreading. This form of spreading expands and carries multiple harm to the victim whose personal, professional and financial life adversely affected.

Mental Impacts

Many studies have been conducted worldwide to find out the mental impact of IBSA on the victim or survivors. Antoinette Huber, a researcher in the United Kingdom, discovered that the majority of women who experienced abuse had at least one mental health condition, either self-identified or diagnosed by a professional.(Huber, n.d., p. 206) Deepfakes raise doubts about the legitimacy of media, leading to confusion. Victims may experience anxiety, depression, and stress due to public exposure of manipulated content.(Brewer, 2019). The psychological problems associated with IBSA include extreme stress, deep depression, intense anxiety including social anxiety, low self-confidence, feeling unsafe, unjustified suspicion, obsessive compulsive disorder, disassociation, somatization, dysfunctional, multiple personality disorder, anorexia nervosa, wide ranging mental health problems, drug abuse, poor adjustment, aggression, and suicidal feelings and behavior. Depressive symptoms are the most prevalent. Another typical side effect is paranoia. The victims were afraid that people in their neighborhood had seen the pictures and would recognize them right away. It was assumed that people were observing them and/or discussing them as a result. This was made worse for women who held jobs requiring direct interaction with the public, such customer service positions. (Huber, n.d., p. 206) The victims of ibsa, need therapeutic intervention in major number of cases. The identification and treatment as a preventive measure needed for victim before the enter the victim- abuser cycle. The health care centres play a crucial role for handling and management of victims.

Physical Impacts

There is a link between the physical and mental health effects on the victims of IBSA. Inadequate mental well-being either caused or contributed to poor physical health. This includes poor eating habits, weight loss, poor personal cleanliness, sleep deprivation, and overall illness.(Huber, n.d., p. 207) The anxiety of whether images or videos would be uploaded or not and whether it has been seen by known person or people identify the victim, caused fear and stress. This fear, cause physical restrains in room or home which adversely affect the physical health of the victim. The fear of identify or teasing by the community made difficult to leave home, they feel home as comfort zone. This physical restraint collapses the everyday task of victim. They avoid the places where perpetrator lives or incidents occurred. They fear even physical violence from the strangers and from the perpetrator again.

Social Impacts

Deepfakes distort public opinion by spreading fabricated news, weakening trust in media and public figures. This manipulation risks harming personal and professional reputations. (Citron & Franks, 2020) The victims of ibsa, are struggle to carry out their day-to-day tasks of life. They fail to concentrate on their work and studies. They prefer to live in a socially isolating condition. They break down social relationship including deleting of social media accounts and would not participate in social events as a decision of social preservation. The fear of whether images would be resurfaced or not is the root cause of social isolation which results in loss of professional and educational opportunities. The social isolation results absences in educational institutions and work place which eventually causes problems in career and community life. Victims suffer from public humiliation and loss of reputation. Trust issues can arise, leading to personal relationships being strained.(McGlynn & Rackley, 2020b) Deepfakes contribute to misleading narratives, erode societal trust, and foster skepticism, especially when public figures are targeted. (Maras, 2020) Affected individuals may face employment termination due to reputational harm. Deepfakes can distort political events, influence voters, and alter election outcomes.

Deepfake Mitigation Frameworks

Deepfakes, as a form of synthetic media, involve altering or creating videos, audio, or images through artificial intelligence, particularly deep learning. These technologies have led to significant societal repercussions. To address these harmful effects, developing effective deepfake detection mechanisms is crucial. However, due to the sophisticated nature of deepfakes, driven by advances in technology, detection methods are becoming increasingly challenging. Therefore, a multi-faceted approach is necessary to effectively identify deepfakes.(Wazid et al., 2024, p. 1)

They are: 1) Educational Initiatives. 2) Regulatory Framework. 3) Technical Solutions. 4) Ethical Concerns. Raising public awareness about the risks of deepfakes is essential to prevent harm. (McGlynn & Rackley, 2020) Legislative and policy measures are necessary to regulate deepfake technology. However, technological advancements pose challenges for law enforcement in combating counterfeit evidence and deceptive material. Effective content removal mechanisms are also crucial. (Citron & Franks, 2020) Current privacy and data protection laws are often insufficient in tackling the range of harms caused by deepfakes. A primary issue is the production and circulation of sexually explicit content without the subject's consent, which raises concerns about privacy, consent, and intellectual property rights. Existing laws are not always designed to address digital alterations of personal images, and intellectual property frameworks are outdated when it comes to the unauthorized use of one's likeness, especially through AI-generated content.

One key challenge is determining who should be held accountable for creating and sharing harmful deepfakes. The responsibility of platforms, such as social media sites, remains unclear. Should these platforms be legally obligated to remove deepfakes proactively, or should they only respond when content is reported? This is a critical issue, as platforms often host and spread deepfake content, yet there is limited legal pressure to monitor and take action unless flagged. AI-based detection methods are critical in identifying deepfakes and reducing their impact on individuals and society. (Maras, 2020) Effective detection of deepfakes requires human ability to distinguish between real and fake content, particularly on social media. Addressing the ethical issues surrounding the creation and use of deepfakes is necessary to ensure responsible technology development and usage. (Franks, 2021)

Legal Outlines in India

India currently has about 850 million internet users, and government estimates indicate that number might rise to 1.2 billion by 2026, making it the largest connected democracy in the world. (Internet in India Report- 2024, 2024, p. 7) According to Government of India policy, every digital nagrik should be able to access the Internet in a way that is "open, safe, trusted, and responsible". (Ministry of Elecs. & Info. Tech. (MeitY), Vision for an Open, Safe, Trusted & Accountable Internet, 2024) Even though, web world gives good outcomes, now the authority has recognized that this same technology can be used as a weapon for criminal activities including deepfakes. (Vaishnav, 2025)

The Indian government has implemented various regulatory frameworks to combat IBSA, particularly the deepfakes. Given the borderless and complex nature of the digital world, where people can communicate instantly and anonymously, there is a global concern over the circulation of false or misleading content, such as deepfakes. In response, the government has taken steps to remove fake clips and promote

awareness regarding the authenticity of digital media.

Technical Measure

- **Blocking of Websites**

The Union Government, through the Department of Telecommunications (DoT), directed Internet Service Providers (ISPs) to block websites listed by the Internet Watch Foundation (IWF), U.K., to stop the sharing of online child sexual abuse material. The Central Bureau of Investigation (CBI), as the national nodal agency for Interpol, is responsible for providing the “Worst-of-List” on child sexual abuse directly to ISPs. (Department of Telecommunications, 2017)

Administrative Measures

- To safeguard the country’s critical information infrastructure (henceforth referred to as CII), the Indian government established the National Critical Information Infrastructure Protection Centre (henceforth referred to as NCIIPC) in compliance with Section 70A of the Information Technology (IT) Act, 2000. Safeguarding CII from unauthorized access, modifications, and destruction is the responsibility of NCIIPC. NCIIPC is responsible for identifying and classifying CII, educating people about threat intelligence and cyber security advice, creating guidelines and standards, and other tasks that are necessary to guarantee a safe, secure, and resilient cyberspace.
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which were issued by the Central Government on February 25, 2021, and later amended on October 28, 2022, and 6.4.2023, impose specific legal obligations on internet service providers, including social media platforms and intermediaries, to ensure their accountability towards a safe and trusted Internet, including their prompt action to remove prohibited misinformation, patently false information, and deepfakes.
- Through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, the Central Government has established standard security practices and procedures for sensitive personal data or information in order to exercise its authority under section 43A of the Information Technology Act, 2000. These rules require that all enterprises that handle or store private and sensitive data have in place appropriate security policies and procedures. (Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, n.d.)
- Government of India, established an Advisory Group consist of government officials, business executives, and academics for the India-specific Regulatory AI framework. Its mission is to encourage innovation while making sure there are sufficient safeguards in place to shield regular people from potential abuse and user harm. In particular, developing

contextualized ethical principles that are flexible in India and support the advancement of reliable, equitable, and inclusive AI is part of the Advisory Group's mandate.(M. Ministry of Elecs. & Info. Tech. (MeitY), 2025)

- In July 2024 and December 2023, the government hosted the Global IndiaAI Summit and GPAI Summit, where a range of government, business, and academic players participated in talks and debates about how to build AI-based solutions in a secure and reliable way. (G. of I. Ministry of Elecs. & Info. Tech. (MeitY), 2024)
- To allow citizens to file complaints against any kind of cybercrime, the Ministry of Home Affairs established the National Cyber Crime Reporting Portal (www.cybercrime.gov.in). It also runs a toll-free helpline (1930). (Ministry of Home Affairs, 2022a)
- The Indian Computer Emergency Response Team (CERT-In) regularly publishes warnings and alerts about the most recent cyberthreats and defenses. Guidelines for protecting IT infrastructure have been released by CERT-In and are accessible on its website. (www.cert-in.org.in).
- The Government of India has established a Grievance Appellate Committee in order to give users and victims the opportunity to appeal decisions made by intermediary Grievance Officers through online at www.gac.gov.in if they are unhappy with the Grievance Officer's decision.(G. of I. Ministry of Elecs. & Info. Tech. (MeitY), 2023)
- The Ministry of Home Affairs (MHA) has opened the www.cybercrime.gov.in portal through which people can lodge complaints about graphic sexually abusive content and child pornography. (Ministry of Home Affairs, 2022)

Suggestive Legal Solutions:

1. Laws should be updated to specifically address the creation and distribution of deepfake content without consent. Individuals should retain control over their likeness and personal data, making the use of someone's image or voice in deepfakes illegal without their explicit approval. This could include expanding the definition of "personal data" to encompass digital reproductions created by AI.
2. Intellectual property laws need to be modernized to protect individuals from the unauthorized use of their likeness in deepfake content. This would involve stronger protections for a person's face, voice, and identifiable features, even when manipulated for new purposes, offering individuals a legal framework to defend their digital identity.
3. Social media and content-sharing platforms should be legally required to implement more effective systems for detecting and removing harmful

deepfakes. These platforms could be mandated to use AI tools to automatically identify and flag deepfakes, similar to existing systems that combat hate speech or misinformation. Failure to address flagged content could result in legal consequences for the platforms, encouraging stricter enforcement of content policies.

4. New criminal penalties could be introduced for the intentional creation and distribution of harmful deepfakes, particularly when used for harassment or defamation. Such laws would serve as a deterrent for those who misuse deepfake technology.
5. Alongside legal measures, public education campaigns could raise awareness about the risks associated with deepfakes and provide guidance on protecting digital identities. By informing individuals about their rights and potential threats, such campaigns could help prevent harm and foster responsible online behavior

Conclusion

The misuse of deepfake technology for creating non-consensual sexualized images represents a significant threat to individual privacy, dignity, and mental health. Combating this issue necessitates comprehensive legal reforms, technological innovations, and educational initiatives to protect potential victims and uphold ethical standards in the digital age. Developing and implementing AI-driven detection tools can help identify and remove deepfake content before it spreads widely. Social media platforms and technology companies must take proactive roles in monitoring and eliminating such content. Raising awareness about the ethical implications and potential harms of deepfake technologies is crucial. Educational programs, especially those targeting youth, can foster digital literacy and promote respectful online behaviour. Providing victims with access to legal aid, mental health counselling, and resources to remove harmful content is essential in mitigating the impact of deepfake abuse.

References:

- Ayub Khan, A., Chen, Y.-L., Hajjej, F., Ahmed Shaikh, A., Yang, J., Soon Ku, C., & Yee Por, L. (2024). Digital forensics for the socio-cyber world (DF-SCW): A novel framework for deepfake multimedia investigation on social media platforms. *Egyptian Informatics Journal*, 27, 100502. <https://doi.org/10.1016/j.eij.2024.100502>
- Brewer. (2019). Revenge Pornography and Mental Health. *Journal of Cyber Psychology*, 19, 220.
- Chaki, D. (2024). MeitY Asks Social Media Platforms to Remove Bomb Hoax Posts, Cooperate with Probes. *Economic Times*. <https://economictimes.indiatimes.com/tech/technology/meity-asks-all-social-media->

intermediaries-to-remove-all-bomb-hoax-content-cooperate-with-probe-agencies/articleshow/114627773.cms. (m.economictimes.com)

Citron, D. K., & Franks, M. A. (2020). The Scourge of Deepfakes: A Technological Approach to Combat Digital Deception. *New York University Law Review*, 95(5), 1076–1104.

Comm. Of Experts on Data Prot., A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. (2018).
https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

Comm. Of Experts on Data Prot., White Paper on Data Protection in India. (2017).
https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_26nov2017.pdf.

Department of Telecommunications, G. of I. (2018). *Government of India, Data on Blocked URLs.*

Department of Telecommunications, M. of C., Government of India,. (2017). *Directions to Internet Service Providers.*

Fido, D., Rao, J., & Harper, C. A. (2022). Celebrity status, sex, and variation in psychopathy predicts judgements of and proclivity to generate and distribute deepfake pornography. *Computers in Human Behavior*, 129, 107141.
<https://doi.org/10.1016/j.chb.2021.107141>

Franks, M. A. (2021). Deepfakes and the Ethics of Consent. *Ethics in Technology*, 35, 51.

Huber, A. (n.d.). *'A shadow of me old self': The impact of image-based sexual abuse in a digital society.*

Information Technology Act, Pub. L. No. No.21 of 2000 (2000).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Internet in India Report- 2024 (p. 7). (2024). Internet and Mobile Association of India.

Kira, B. (2024). When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act. *Computer Law & Security Review*, 54, 106024.
<https://doi.org/10.1016/j.clsr.2024.106024>

Lok Sabha Secretariat, S. Q. No. 142. (2019). *Proposed Amendments to Intermediary Rules.* <https://sansad.in/getFile/loksabhaquestions/annex/17/AS142.pdf>. (Digital Sansad)

Maras, M. H. (2020). Deepfakes and the Law. *Harvard Journal of Law and Technology*, 44, 132.

McGlynn, C., & Rackley, E. (2020a). Non-Consensual Image-Based Sexual Abuse. *Feminist Legal Studies*, 28, 225.

McGlynn, C., & Rackley, E. (2020b). Non-consensual Image-Based Sexual Abuse: The Rise of Deepfakes and Digital Harassment. *Feminist Legal Studies*, 28 (4), 225–242.

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond ‘Revenge Porn’: The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies*, 25(1), 25–46. <https://doi.org/10.1007/s10691-017-9343-2>

Ministry of Elecs. & Info. Tech. (MeitY), G. of I. (2023). *MeitY Launches the Grievance Appellate Committee (GAC)*. <https://pib.gov.in/PressReleasePage.aspx?PRID=1903118>.

Ministry of Elecs. & Info. Tech. (MeitY), G. of I. (2024). *Global India AI Summit 2024: Shaping the Future of AI*, Press Release. <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2030838>.

Ministry of Elecs. & Info. Tech. (MeitY), M. (2018). *Draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018*. https://prsindia.org/files/bills_acts/bills_parliament/2021/public_comments_draft_intermediary_guidelines_rules_2018.pdf. (PRS Legislative Research)

Ministry of Elecs. & Info. Tech. (MeitY), M. (2019a). *MeitY Invites Counter Comments/Suggestions by 14 Feb 2019 on Draft Intermediary Guidelines*. <https://lexplosion.in/meity-invites-counter-comments-suggestions-by-14th-february-2019-on-draft-intermediary-guidelines/>. (Lexplosion)

Ministry of Elecs. & Info. Tech. (MeitY), M. (2019b). *MeitY Seeks Public Comments on Changes to IT Rules*. <https://www.medianama.com/2019/01/223-meity-it-rules-public-comments-2/>. (MEDIANAMA)

Ministry of Elecs. & Info. Tech. (MeitY), M. (2024). *Press Note on Data Protection Provisions in the IT Act*. https://www.meity.gov.in/writereaddata/files/press_note_data_protection_ITAct.pdf.

Ministry of Elecs. & Info. Tech. (MeitY), M. (2025). *Government of India, Report on AI Governance Guidelines Development*. <https://indiaai.gov.in/article/report-on-ai-governance-guidelines-development>

Ministry of Elecs. & Info. Tech. (MeitY), Vision for an Open, Safe, Trusted & Accountable Internet. (2024). [Annual Report 2024-25]. Government of India.

Ministry of Home Affairs, G. of I. (2022a). *Cyber Frauds Helpline*. <https://pib.gov.in/PressReleasePage.aspx?PRID=1814120>.

Ministry of Home Affairs, G. of I. (2022b). *National Cyber Crime Reporting Portal*. <https://cybercrime.gov.in/>.

Office Memorandum, No. 3(6)/2017 Cyber L. Div. (2017).

Oxford Learner's Dictionaries. (n.d.). Oxford University Press. Retrieved February 13, 2025, from <https://www.oxfordlearnersdictionaries.com/definition/english/deepfake?q=deepfake>

Sparks, B., Stephens, S., & Trendell, S. (2023). Image-based sexual abuse: Victim-perpetrator overlap and risk-related correlates of coerced sexting, non-consensual dissemination of intimate images, and cyberflashing. *Computers in Human Behavior*, 148, 107879. <https://doi.org/10.1016/j.chb.2023.107879>

The Hindu, C. A. (2018). *Cambridge Analytica Data Scandal: Govt. Seeks Explanation from Facebook*. <https://www.thehindu.com/news/national/cambridge-analytica-data-scandal-govt-seeks-explanation-from-facebook-ca/article23384711.ece>.

Vaishnaw, A. (2025, January 15). *Keynote Address at Digital India Dialogue* [Keynote Address]. Digital India Diakogue.

van der Sloot, B., & Wagenveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. *Computer Law & Security Review*, 46, 105716. <https://doi.org/10.1016/j.clsr.2022.105716>

Vinayak, V., & Bhatia, R. (2020). Understanding the Psychology Behind Deepfakes: A Study on Human Behavior and Technological Manipulation. *Journal of Technology and Human Behaviour*, 19 (2), 54–68.

Wadden, K., & Dain, K. (2019). The Addictive Nature of Deepfake Technology and its Psychological Impact. *Journal of Cyber Psychology*, 34 (3), 145–158.

Wazid, M., Mishra, A. K., Mohd, N., & Das, A. K. (2024). A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact. *Cyber Security and Applications*, 2, 100040. <https://doi.org/10.1016/j.csa.2024.100040>