DEEP FAKES AND THE CRISIS OF KNOWING: A COMPARATIVE STUDY OF THE INDIAN AND UK LEGAL FRAMEWORKS

Heena Narwani & Aditi Kanoongo, Assistant Professor, S.S. Jain Subodh Law College

ABSTRACT

Deepfake, which refers to a synthesized audio-visual medium that has been created or modified via deep learning technology with the aim of making it appear real, has become a structural challenge to the epistemic commons insofar as it refers to a shared level of trust that makes audio-visual evidence credible in the eyes of individual citizens, media, and electorate. This epistemic crisis takes two forms: first-order harm, which includes defamatory, sexually exploitative, fraudulent and manipulative electoral activities brought about through fabricated content being believed; and second-order harm through 'liar's dividend', wherein authentic evidence may be disregarded as deepfake. This paper seeks to undertake a doctrinal and comparative examination of the Indian and UK responses to this challenge. The Indian response is essentially executive and reactive, centered on amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, in 2025 and which provides for statutory definition of 'synthetically generated information' and labeling and takedown requirements, among others. The United Kingdom has taken steps through legislative amendments to primary statutes, the Online Safety Act 2023 and the Data (Use and Access) Act 2025, criminalizing firstly the distribution and secondly, from February 2026, the production of non-consensual sexually explicit deepfakes with the assistance of Ofcom's regulatory powers. This paper posits that in both jurisdictions there is a reactive approach and an emphasis on sexual harm, resulting in considerable regulatory deficiencies concerning deepfakes that are not sexual, political, economic and reputational in nature and makes recommendations for reform in this regard.

Keywords: deepfakes; synthetic media; epistemic harm; Information Technology Act; Online Safety Act 2023; personality rights; comparative media law; artificial intelligence regulation.

INTRODUCTION:

The rapid development of Artificial Intelligence has significantly transformed the manner in which information is created, communicated and consumed. This progressive development of Artificial Intelligence and machine learning has led to the mix of effects which are interesting, revolutionary and disruptive. One such deeply disturbing phenomenon is the rise of Deepfakes. The term "deepfake" consist of two words "deep learning" and "fake". It is defined as the synthetic media which involves the digital manipulation of original source material and is intended to deceive.[1] In simple words, it is a digital content which has never happened before and is merely a figment of creativity. This term was first used in 2017 on Reddit to refer explicit videos shared on the platform using open-source face-swapping technology.[2] But, recently, its scope has been widened to include any digital media that has been created or altered using AI in a way that superimposes the video or audio likeliness of one person or thing over another. The technology behind this extraordinary phenomenon is known as Generative Adversarial Networks, a machine learning framework that pits two neural networks against each other - one generates synthetic data, while the other tries to distinguish it from real data. The malicious applications of deepfakes are manifold and concerning, as they can be used to create false narratives, discredit public figures, perpetrate financial fraud, and even produce non-consensual explicit content.[3]

The potential threat posed by deepfakes is of significant concern as their harms operate across various legal domains. It leads to the infringement of an individual's privacy by using their face, voice or image without assent, it may lower reputation through fabricated statements or conduct, it may result in increased crime of identity theft and financial frauds and may also affect the integrity of digital evidences. Consequently, deepfakes cannot be comprehensively analyzed in terms of a "fake news" or Internet misinformation problem. Rather, deepfakes should be viewed as a complex legal issue that arises at the nexus of artificial intelligence technology, privacy, dignity, freedom of speech, criminal law, intermediary liability, intellectual property rights, data protection law, and evidence law.

The statutory reaction to the deepfakes in India has been shaped in line with an interaction of

[1] Deep Fake, WESTLAW, https://us.practicallaw.thomsonreuters.com/w-039- 7965 (Last accessed August 5, 2026).
[2] Meredith Somersn 'Deepfakes, Explained' (MIT Management Sloan School, 21 July 2020) accessed 6 August 2026.
[3] Krishang and Aastha, "Deepfake Crimes and Legal Regulation in India", IJCRT Volume 13 Issue 3, Page 150.

the existing legislation with certain developments in the field rather than a single deepfake legislation in the country. This includes the Information Technology Act, 2000 which constitutes the main legal framework that addresses various illegal acts in the cyberspace including identity theft, breach of privacy, sexual explicit material, and intermediary liabilities. Another piece of legislation, which is the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 outlines the due diligence obligations of intermediaries as well as the mechanism for addressing illegal material posted in the internet. India has recently made great strides in deepfakes regulation through amending the IT Rules on Synthetically Generated Information (SGI) through 2026 amendment.[4]

The United Kingdom offers a valuable comparative jurisdiction in this regard. Unlike in India, the UK has managed to create a relatively sectoral and harm-based legal regime regulating online harms through various laws. In particular, the Online Safety Act 2023 is the central element of the UK's online safety regime imposing obligations on regulated online services regarding illegal content and user safety. However, the UK legislation should also be taken into account in relation to sexually explicit deepfakes and intimate image offences since recently there have been new developments of a regulatory nature intended to regulate AI generated intimate images and technologies employed to distribute them. Several important aspects of comparing the Indian and UK approaches exist. First, the two approaches try to strike a balance between the interests of privacy, dignity, security, free speech, and innovation using different institutional and regulatory means. While the Indian approach incorporates the interplay of constitutional principles, Information Technology Act, intermediary liability, criminal, evidence laws, and newly emerging regulation of SGI, the UK approach consists of human rights, online safety, criminal, data protection, and regulatory law. However, both approaches fail to address the epistemic problem created by SGI.

CONCEPTUALISING DEEP FAKES:

2.1. Meaning of Deepfake:

The term “deepfake” has no statutory definition in Indian laws. But, it can be understood as a synthetic or artificial generated audio or video of real individuals with respect to events that

[4] Suruchi, “*Deepfakes and the Law: A Comprehensive Comparative Analysis of Indian and International Legal Frameworks*”, Indian Journal of Law and Legal Research, Volume 7 Issue 5 , Page 3535.

has never happened. The USA law on deepfakes Accountability Act, 2019[5] defines "deepfakes as any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof—

"(A) which appears to authentically depict any speech or conduct of a person who did not in fact engage in such speech or conduct; and

(B) the production of which was substantially dependent upon technical means, rather than the ability of another person to physically or verbally impersonate such person."[6]

What sets the deepfake apart from all other forms of digital media manipulation, such as image alteration using Photoshop or computer generated imagery (CGI), is that deepfakes generate their images using an artificial intelligence based model trained on vast data sets of the subject's image, thus providing photorealistic imagery and motion coherence beyond the scope of conventional editing techniques.

2.2. Historical Evolution of Deepfake:

The theoretical and technical background behind deepfakes is traceable even before the emergence of the concept of the deepfake in the past several decades. Digital manipulation of images and videos can be traced back to as early as the 1990s where the emergence of software like Adobe Photoshop (1990) allowed for highly realistic modification of images, and CGI and motion capture "de-aging" or face replacement technology became a necessity in big budget movies in the 2000s. The aforementioned technology, however, involved a lot of laborious effort and specialized software along with costly computer power making the practice exclusive only to the studios and amateur image makers. It was not until 2014 that the technical innovation occurred, when Ian Goodfellow and collaborators proposed the architecture of the generative adversarial network (GAN), where two neural networks, the first creating artificial images and the second attempting to discern whether an image is real or fake are taught to compete with each other until the generator creates something that becomes almost indistinguishable by the discriminator and even by a human. Over the course of the next three years, the architecture of GANs and autoencoders has been used to create videos with face

[5] H.R. 3230, 118th Congress (2023) https://www.congress.gov/bill/118th-congress/house-bill/5586/text Last accessed on 7 August 2026.
[6] S Nivedha, Samanvitha Murali, "*Deepfakes in India: Unraveling India's Legislative Uncertainty and Jurisdictional Dilemma*", TIJER, Volume 11 Issue 11, Page a612.

swaps, resulting in the coinage of the term "deepfake" in late 2017 when the first pornographic videos featuring swapped faces of celebrities were uploaded to forums using open-source software[7].

The years between 2018 to 2020 saw extensive growth in deepfake technologies and their uses, alongside the emergence of the initial legislation and platform reactions to them. Accessible mobile apps (such as face-swap apps or "reface" apps) have allowed average users to use adjacent capabilities of deepfakes, while state and non-state actors have begun experimenting with them for spreading disinformation, such as 2018's fake video of a former US President that was done to illustrate the dangers of this technology to the public. This period also witnessed the emergence of the first legislations against deepfakes, namely those in 2019 which have been passed in two US states California and Texas, in response to deepfake electoral content and non-consensual pornography respectively, and in China disclosure requirement of AI-created content. The shift from static, pre-recorded deepfake content to real-time, interactive synthetic audio and video capable of sustaining a live conversation or video call represents the most recent and, from a regulatory standpoint, most challenging phase of the technology's evolution, as it substantially narrows the window available for detection, verification, or intervention before harm occurs. It is this most recent phase that has principally driven the 2023–2026 wave of legislative activity examined in this paper, including India's 2025 IT Rules amendment and the United Kingdom's 2023–2025 amendments to the Sexual Offences Act 2003.

2.3. Types of Deepfake:

Deepfakes are a varied type of synthetic media. The developments in the realm of artificial intelligence have made possible manipulation or creation of various aspects of human identity and communication through audiovisual means such as facial features, voice, expressions, body language and whole environments. For legal analysis, the categorization of deepfakes plays a crucial role as different forms of manipulation might result in different forms of legal damage. Copyright or personality rights and consent issues may arise from the use of face-swap technology to produce an entertaining video. Meanwhile, privacy and dignity problems can be caused by a synthetic intimate video.

[7] Suruchi, "*Deepfakes and the Law: A Comprehensive Comparative Analysis of Indian and International Legal Frameworks*", Indian Journal of Law and Legal Research, Volume 7 Issue 5, Page 3535.

1. **FACE-SWAP DEEPFAKES:** Face-swapped deep fakes represent the oldest and, in the eyes of the public, to this day, the most representative type of deep fake media. This method is based on the digital placement of the face of an identifiable person on the body of another person using pre-existing video/image footage, where the process of generating this new imagery is done via autoencoder networks or GANs trained on a collection of images of the desired face[8].

2. **AUDIO DEEPFAKES/VOICE CLONS:** It means synthetic reproduction of the voice, tonality, cadence, and manner of speaking of the target based on an authentic audio sample, where, with the aid of current technology, this audio clip need not even be more than three to ten seconds in length, with the source being any type of public speech like a voice mail message, video footage from social media, or a conference call. Voice cloning is now the fastest growing vector of deepfake scams and frauds that involve voice impersonation of a family member or business executive[9].

3. **FULL-BODY AND GESTURE DEEPFAKES:** Deepfakes of full-body and gestures take manipulation further than the face by reproducing the entire body, its stance, gait, and bodily movements of a person through the use of motion capture data or pose estimation algorithms trained on videos of the target so as to transfer the unique bodily style of the target to either a new body or a completely synthetic one. In contrast to face-swapping and reenactment methods where facial changes are made but a new body is used, such deepfakes create a full bodily image and are more useful in recreating a target performing activities that never happened.

4. **TEXT-BASED AND MULTIMODAL SYNTHETIC CONTENT:** It includes written statements generated by AI that are wrongly credited to a specific individual or a combination of synthetic writing, image, and voice, such as a synthesized "leaked" chat transcript and voice note, make up a new form of hybrid fraud not well covered by present legal terms that focus on "image," "video," or "recording."

CONCERNS POSED BY USE OF DEEPFAKES:

The spread of the use of the technology of deepfakes raises questions at the personal,

[8] Anuragini and Shobanal, "*A socio Legal Enquiry on Deepfakes*" 54 Calif. W. Int'l L.J. 517 (2024).
[9] Palak Rajpal, "Navigating the Socio-Legal Implications of Deepfakes: A Comparative study"998 Advances in Soc. Sci., Educ. & Humans. Rsch. 162 (2026).

institutional, and systemic levels, and the understanding of such questions is required for the proper evaluation of any regulatory framework.

From the perspective of an individual person, the first issue arising is related to issues of privacy, dignity, and consent. Sexual deepfakes produced against the will of individuals cause psychological damage, damage to reputation, and even physical harm, which can be compared to and even be greater than the one inflicted by the unauthorized circulation of actual nude pictures. Indeed, in addition to the damage mentioned above, the victims have to face the fact that what was depicted did not actually happen, but still looks credible to the viewers and cannot be removed after being posted.[10]

On the economic front, deepfake based fraud has turned out to be one of the fastest-growing types of criminal acts. Voice cloning and video impersonation are increasingly being used for defrauding corporations, banks, and individual consumers, with losses amounting to millions per incident, as in the Arup Hong Kong case, and with identity verification processes that rely on facial or voice biometrics now deemed insufficient on their own. Small and medium-size businesses, which do not have the same verification processes as larger companies, find themselves especially vulnerable to such scams, while fraud and cheating laws in both India and the UK, although technically relevant, did not take into account the speed and sophistication of AI-powered deception.

On the institutional and democratic level, deepfakes represent a different type of threat. Fake statements or behaviors of a political candidate or official can spread widely before any checks could be done, especially in the compressed timeframe of an electoral race, while even the threat of such deception has been shown to reduce trust in campaign materials both genuine and fake which represents the 'liar's dividend' mentioned in Section 2.Neither India nor the UK has adopted any specific deepfake based electoral laws, leaving such an act to be punished via general election related, defamation, and false communication laws.

Yet another, cross-cutting issue relates to detection and forensic verification. Humans do poorly in recognizing deepfakes with complex layers of manipulation, with tests indicating human error rates in detection that may be as high as only a few tenths of one percent, and automated systems facing an endless game of cat-and-mouse as they try to detect the latest

[10] Ankita Khamari, "The Rise of Deepfake Technology: Societal, Ethical and Legal Challenges in The Digital Age", 2 Int'l J. for Legal Res. & Analysis, no. 7 (2025).

generative models used for deepfakes, making any detection technique rendered ineffective in as little as several months after its initial success. Neither of the jurisdictions discussed in this paper has an independently mandated forensic authority which can definitively establish whether disputed content is authentic or synthetic.

Finally, the regulation of deepfakes is a challenge to free expression. Legislation or regulations which are sufficiently broad to cover the latest generative techniques may end up covering legitimate instances of satire, parody, political comment, and artistry, especially when a regulator or a platform is expected to quickly determine whether content is authentic and has an intended purpose. This balance between breadth and potential overreach is an issue throughout the comparative discussion in this paper, most notably in light of the broadly drafted 2025 IT Rules amendment

EXISTING LEGAL FRAMEWORK IN INDIA:

There is no dedicated law against deepfakes in India. Rather, there is an ad hoc approach to the law based on provisions of the Constitution, Information Technology Act, 2000, and the Rules under it, the Bharatiya Nyaya Sanhita, 2023, Digital Personal Data Protection Act, 2023, and the Copyright Act, 1957. Every one of these statutes is applicable to merely a portion of the deepfake menace, as explained below:

4.1. Right To Privacy and Constitutional Dimension:

The constitutional basis for seeking remedy for deepfake incidents in India is, first and foremost, Article 21 of the Constitution of India, which provides for the right to life and personal liberty and, judicially, extends the right to privacy, dignity, and reputation. In the seminal decision of **K.S. Puttaswamy v Union of India (2017)**[11]a nine-judge bench of the Supreme Court held unanimously that the right to privacy is a fundamental right that inheres in Article 21, which covers informational privacy and bodily integrity a ruling highly relevant to the issue of deepfakes, as the creation of synthetic sexual or defamatory material with the use of a person's image without their consent is a classic case of infringement of both aspects of the right to privacy articulated in that ruling. The right to reputation has also been read into Article 21 in subsequent cases, thereby providing another constitutional base for remedy for

[11] Justice K.S. Puttaswamy(Retd) v. Union of India, AIR 2018 SC (SUPP) 1841.

individuals suffering from the fabrication of defamatory content based on their likeness.

Article 19(1)(a), which protects the freedom of speech and expression, may conflict with the interest in privacy and dignity as the regulation or removal of synthetic content involves restrictions on the exercise of this freedom, including, possibly, lawful satire and commentaries. Article 19(2) allows reasonable restrictions on this right for purposes including, inter alia, decency, morality, defamation, and public order rationales commonly used for intermediaries' takedown obligation for deepfakes, especially after the amendment of IT Rules in 2025[12]. In addition to that, Article 14 of the Indian Constitution, which guarantees equality before the law, has been used in legal scholarship to challenge the potential arbitrary and unequal use of the broad and vague authority of the government officials to order takedown of 'synthetically generated information' under the amended Rules. This constitutional context must be taken into account when interpreting the statutory provisions described below, but does not itself provide any enforceable remedy an individual cannot bring a suit based on Article 21 alone, as the Constitutional right needs an actionable statutory or common law ground behind it.

4.2. Information Technology Act:

The IT Act continues to be the special legislation for digital content in India and contains various provisions of incidental application to deepfakes. Section 66C punishes identity theft for the fraudulent or dishonestly obtaining or using another person's electronic signature, password or any other kind of unique identification mark, and this provision has been relied upon in interpreting that deepfakes could fall within this section. Section 66D punishes cheating by personation using computer resources, and is thus directly relevant to deepfakes when used for impersonating someone for fraudulent purposes. Section 66E punishes capturing, publishing or transmitting any image of a person's private parts without the person's consent and in circumstances of violation of privacy, which may be relevant to some non-consensual deepfakes in the category of sexual deepfakes, although whether this provision applies to synthetic images of such a nature is open to debate. Sections 67 and 67A respectively punish the publication or transmission of obscene or sexually explicit material, and these sections have traditionally been used for prosecuting non-consensual sexual deepfakes in the

[12] Sree Parvathavarthini SK & Santosh Kumar Tiwari, Deepfake Technology: Legal Challenges and Regulatory Responses, 6 Indian J. Legal Rev. 774, 777 (2026).

absence of specific legislation for such deepfakes.[13]

In terms of subordinate legislation, however, perhaps the Act's most recent and important development pertains to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended from 15 November 2025 onwards. These rules have for the first time provided a statutory definition of the term 'synthetically generated information', under Rule 2(1)(wa), referring to content which is artificially or algorithmically generated or modified by the use of a computer resource in such a way as to appear reasonably authentic. Social media intermediaries are now mandated to make users notify whether such content is being published, identify it as synthetically generated, and attach relevant metadata labels to at least ten per cent of the visual screen space (or make an audio announcement for audio content). This amendment no longer requires the intervention of a court order or a government notification for takedowns; significant intermediaries shall themselves take down unlawful synthetically generated information, failing which they will lose the benefit of safe harbour provisions in Section 79 of the IT Act, while the power of issuing takedown orders has been limited to officials at joint secretary level or higher in the government and deputy inspector general level or higher in the law enforcement agencies.

4.3. Bhartiya Nyaya Sanhita:

In its place, the Bharatiya Nyaya Sanhita, 2023 ('BNS'), which came into effect on 1 July 2024, contains several general provisions that can potentially be used to prosecute deepfakes. Section 318 sets out the general offence of cheating, while section 319 criminalizes 'cheating by personation' acting as another person real or fictional with the intention of deceiving, for which an offender can be imprisoned for up to five years, a provision particularly relevant to those who use deepfakes to impersonate someone for fraudulent purposes. Section 336 provides for forgery, including forgery of electronic records, a provision relevant to the fabrication of digital documents or communication using artificial intelligence. Section 351 makes it an offence of criminal intimidation, relevant to situations where a threat to publish or distribute a deepfake is made unless a certain demand is met (so-called 'deepfake sextortion'). Section 353 provides for the publication of misleading information likely to cause fear or public alarm, a provision which could potentially be relevant in cases where deepfakes are being used for political purposes. Section 356 provides for the offence of defamation, where a morphed or artificially

[13] Shinu Vig, Regulating Deepfakes: An Indian Perspective, 17 Journal of Strategic Security, 82 (2024).

created image or video that is damaging to someone's reputation can be criminalized irrespective of whether the underlying image or video content was created with the help of AI tools. Chapter XV of the BNS on offences against public decency and morals remains relevant to the creation and dissemination of obscene synthetic material as it did previously under the Indian Penal Code. It is generally condemned, however, as a misapplication of general-purpose provisions that were not tailored with synthetic media in mind. The concepts of dishonest intent, personation of a particular person, and publication in a public place were not intended for a situation where the wrongdoer may be anonymous, outside the jurisdiction, and creating something that shows no real act committed at all.

4.4. Digital Personal Data Protection Act:

The Digital Personal Data Protection Act, 2023 ('DPDP Act') controls the processing of personal data, including biometric identifiers in the form of the individual's facial geometry or voice print that serve as the basic elements of the majority of deepfakes. According to the Act, personal data can only be processed for a lawful purpose and with the consent of the data principal unless there are certain exceptions, and there is also a Data Protection Board that can conduct investigations and impose fines for the lack of compliance. In the case when an individual's photographs, videos or voice recordings are scraped from social media or other sources without consent for training and fine-tuning a generative model with the aim to produce a deepfake, this could be considered unauthorized processing of personal data and thus violate the provisions of the Act concerning consent and purpose limitation, and provide another but as of now quite untested avenue of addressing deepfake cases aside from those discussed above. However, the application of the DPDP Act as a means to protect deepfake victims is limited by the lack of specific provisions on deepfakes, as well as by the difficulty of determining the 'data fiduciary' in the case in question.

4.5. Copyright Act:

The Copyright Act, 1957 is of merely an indirect and incomplete nature when it comes to dealing with the issue of deepfakes because it deals with the protection of original literary, dramatic, musical and artistic works and cinematographic films, and not with the personal image, voice or identity of a person as such. However, there are two provisions in the said Act which may have some indirect bearing on this issue. First, Section 38 of the Act gives performers' rights, which enables them to prevent the unauthorized reproduction or

communication of their performance in case a deepfake involves any such unauthorized use of an actual performance which is copyrighted. Second, under Section 57 of the Act, the author of a work is entitled to a certain special right, which is often referred to as "moral right" to claim authorship of a work and also prohibit any distortion, mutilation or modification thereof in any manner which is prejudicial to his honor or reputation; however, it has been applied in certain personality-right cases involving unauthorised manipulation of a person's recorded image or performance only by way of analogy, and can be exercised by a claimant only in relation to a work in which he owns the copyright or performer's right.

4.6. Flaws in the Current Legal Framework:

A. **Lack of specific legislation:** The regulation of deepfakes in India is achieved by interpreting the constitution, utilizing general provisions of criminal law, data protection laws, incidental copyright doctrines, and executive rule-making without any particular statute regulating offenses, defenses, or remedies relating to deepfakes, despite the pending Regulation of Deepfake Bill, 2025.

B. **Overreliance on general principles poorly designed for deepfakes:** The BNS provisions on cheating, personation, forgery, intimidation, and defamation have been framed without considering synthetic media, thereby necessitating the use of doctrinal elements such as dishonest intent and identifiable personation to cover conduct involving anonymous and AI generated content.

C. **Differential access to remedy:** Protection of personality and publicity rights through judge-made laws has evolved exclusively by the decisions of Delhi High Court cases which realistically can be pursued only by wealthy celebrities and public figures.

D. **Lack of forensic infrastructure:** There is currently no statutory provision for an independent forensic entity in India to authenticate the disputed information as either genuine or fabricated, thus limiting both criminal prosecution and civil remedy irrespective of the substantive law applicable.

E. **Biased toward sexual harm and celebrities:** The current legal regime, including case law on personality rights and the provisions against obscenity under the IT Act

and BNS, focuses heavily on non-consensual sexual content and celebrities, leaving other forms of fraudulent, political, and defamatory deepfakes somewhat neglected despite statistics indicating that there is an increasing number of cases belonging to the latter three categories of harm.

F. **Free-expression implications of overbreadth:** The very wide definition of "synthetically generated information" proposed in the 2025 IT Rules amendment could lead to the restriction of satire and political comments as there is currently no statutory exceptions, which was raised as a concern by digital-rights advocates during the legislative process of the amendment.

G. **Problematic data fiduciary duties under the DPDP Act**: The DPDP Act fails to outline which actor in the supply chain of the generative AI — either a model developer, platform owner, or an end-user — would be obligated to fulfill data fiduciary duties in case when a deepfake is generated using scraped biometric data.

H. **Lack of cross-border enforcement mechanism:** Deepfakes are often created and disseminated from foreign jurisdictions and there is currently no mutual legal assistance or cross-border takedown provisions in any of the statutes discussed above.

EXISTING LEGAL FRAMEWORK IN UK:

As in India, there are no clear-cut laws about deepfakes in the UK as well. The regulations came through the changes made to the existing laws, especially when it comes to deepfakes that contain sexually explicit content. It is completely up to what the image contains for the image to be seen as illegal under UK laws. Deepfakes are not necessarily illegal per se, but they fall under the same rules as photographs that contain prohibited images. Sexual Offences Act 2003 is the primary legal framework concerning sexual offences in UK. It is pertinent to note that Section 188 of the Online Safety Act 2023 amended Section 66B of the Sexual Offences Act 2003 to introduce an offence regarding non-consensual sharing (or even threatening of sharing) of the intimate image, being written in such a way to encompass images which only 'appear to show' a particular person in an intimate situation, hence extending the current law against intimate-image abuse to include deepfakes regardless of whether any sexual activity took place or not; the amendment entered into force on 31 January 2024. Still, it dealt

with dissemination but did not encompass creation of such images within the scope of the act.

The above-discussed loophole was filled by the Data (Use and Access) Act 2025. Section 138 of the Act amended Sexual Offences Act to make it an offence to deliberately create ‘a purported sexual image of another person’ without their consent, both using AI and other methods of manipulating the image; the offence entered into force on 6 February 2026.

Without reference to the intimate-image-abuse issue, those who are victims of UK deepfakes can rely on the general law of defamation, malice falsehood, harassment under the Protection from Harassment Act 1997, misuse of private information, and data protection laws, which, as opposed to Indian jurisprudence of personality rights of celebrities, in principle, are available to everyone, although there are challenges related to cost and the problem of tracing the author of the content in both jurisdictions.

One of the notable pieces of legislation governing deepfakes involving children in UK is the Protection of Children Act 1978. This Act deals with indecent images of children. In essence, this Act relates to the creation of any digitally produced images that appear to depict a child. Thus, the use of AI 'nudification' applications for producing indecent images depicting children may incur criminal liability, irrespective of the fact that the image is not a real one.

Recently, the Crime and Policing Act 2026 was passed in the UK that strengthens the legal regime there. This act introduces new offences relating to tools, programs, and services used for the production of non-consensual intimate images. Under Section 99 of Crime and Policing Act, an offense of using AI tools for creating images that are false and sexually explicit or nude is criminalized. This offense criminalizes the provision and distribution of artificial intelligence software meant to create false naked pictures of real persons. Instead of criminalizing individual use of deepfake, the law addresses the technological and economic infrastructure used in making such offenses possible. Another feature under the act is removal of intimate images as fast as possible, but not later than 48 hours after filing a complaint.

Therefore, the UK's approach in regulating deepfake images has changed from sharing of these images to the creation of deepfakes to finally targeting AI technology and infrastructure used in their creation.

COMPARATIVE ANALYSIS:

These two approaches to deepfake regulation are separated by many dimensions which have been captured in Table 1. First of all, there is a difference in the way India and the United Kingdom regulated deepfakes. India mainly used the constitutional interpretation, general criminal laws and data protection laws, as well as delegated executive regulations pursuant to the IT Act, while the UK regulated deepfakes through the amendment to the relevant primary legislation, which, however, took place very slowly but produced a very robust effect and more focused approach to the problem than the Indian way, at least until now.

Dimension	**India**	**United Kingdom**
Primary means of Regulation	Executive rule-making pursuant to the IT Act, 2000 (IT Rules 2021, amended 2025); no stand-alone law.	Online Safety Act 2023 and Data (Use and Access) Act 2025, amending the Sexual Offences Act 2003
Issues of Conduct involved	Labelling, disclosure, and intermediaries' takedown of "synthetically generated information" in general (and not necessarily involving sexuality)	Traditionally restricted to the dissemination of sexually explicit deepfakes; production prohibited only from February 2026
Core Mechanism	Due diligence and safe harbour conditionalities of Section 79 IT Act;	Criminal offence and responsibilities of OfCom as a regulator.
Regulator	Ministry of Electronics and Information Technology (MeitY)	No independent AI or content regulator. Ofcom as per statutory codes of practice of the Online Safety Act
Creation and/or circulation of non-consensual intimate imagery	Indirectly covered by obscenity laws and sections of the IT Act and the Bharatiya Nyaya Sanhita, 2023	Explicitly criminalized sharing and creation of purported sexual images.

In terms of functional design, India's approach has wider scope in the matter area but lesser depth in remedial action, with labelling and removal of offending content on platforms instead of individual-specific criminal or civil relief available to ordinary individuals. On the other

hand, the UK's approach has more narrow scope in the matter area but greater depth in the form of specific crime, custodial as well as forfeitures of devices and registration with Sex Offenders Register when the case is severe enough. However, neither country has managed to craft a legal framework wherein the epistemological aspect of deepfake has been taken as a separate matter for regulation.

CONCLUSION:

The cases of India and the United Kingdom show two different regulatory approaches to the same basic problem. India's amendment to the 2025 IT Rules has broad coverage pertaining to technology neutral definition of all synthetic media but a relatively shallow set of remedial mechanisms based on platforms. Meanwhile, the amendments to the Sexual Offences Act 2003 introduced in the United Kingdom have created a proper criminal offense with substantive sentencing implications and exclusively target sexually explicit material. Neither regime, however, addresses the epistemic harm caused by deepfakes, particularly the erosion of trust in audio-visual evidence, as a distinct object of legal regulation. As generative AI develops faster than legislation and case law, the remedy to this problem will require shifting from individual to systematic interventions in relation to the origin of the content, its forensic verification and international enforcement of the law, in order to deal not only with the victims of a particular deepfake but also with the general problem of epistemology created by them.