**International Journal of Law, Policy and Social Review**
**www.lawjournals.net**
**Online ISSN: 2664-6838, Print ISSN: 2664-682X**
**Received: 13-08-2025, Accepted: 12-09-2025, Published: 27-09-2025**
**Volume 7, Issue 3, 2025, Page No. 117-127**

# Legal implications of deepfake technology: Addressing the efficiency of current law in addressing deepfake

**Lakshika Negi**
Department of Law, Chandigarh University, Chandigarh, Punjab, India

**Abstract**
Technology by taking the help of artificial intelligence to create hyper- realistic fake media, has evolved significantly since its inception, drives by advertisement in machine learning and computer graphics. This research paper explores the introduction of the deepfake, their evolution, benefits, and threats as well as the legislative framework surrounding their use and suggestions for future governance. In the introduction of deepfake technologies marked a paradigm, shift in media manipulation, enabling the creation of video and audio that can convincingly depict the individuals in fabricated scenarios. As the technology has evolved, it has found application across various sectors, including entertainment, offering innovative ways to engage audience and enhance still telling.

The proliferation of deepfake poses substantial threats, particularly in the realms of misinformation privacy violation, and potential harm to individual's reputation. The ability to create realistic, yet deceptive content raises the ethical concern and challenges the integrity of information in the digital age. In respond to these threat, various legislative frameworks have emerged globally, to address, misuse of technology. These regulations seek to balance innovation with the protection of individual and society from harmful application.

To effectively navigate the complexity of the deepfake, suggestions of a comprehensive approach include promoting digital literacy, enhancing detection technology, and establishing clear guidelines for ethical usage. In conclusion, while deepfake technology present exciting opportunities, it also damages, careful consideration of its implementations. A protective and collaborative approach involving policymakers, technologist, and the public in essential to harness the benefits of deepfake while mitigate their risk.

**Keywords:** Deepfake, Fabricated, synthetic, artificial intelligence, technology, fake, threats, realistic

## Introduction

The earliest example of fake news appeared in the 13th century BC, when Rameses the great spread lies and propaganda portraying the Battle of Kades as stunning victory while the battle actually ended in a stalemate. Various other examples of fake news appear over the centuries but its use become widespread in the 1900s when it was used as a form of propaganda during the both world war I and II. By the passage of time the technology become advance and the fake information turns to the deepfake causing greatest harm to the person**,** going through the same battle Rashmika Mandanna's deepfake video, which was made with the help of the AI, went viral on social media in the November 2023. Walking on the same path on April 2018 a video bloomed on the WhatsApp, world's most popular message platform. The footage apparently from the CCTV camera, showing a group of the children enjoying cricket in the street. Suddenly two men on bike grab one of the smallest kids and speed away. This kidnapping video cause widespread confusion and panic in the society, which result in 8-week period of mob violence that kills at least 9 innocent people. The footage that sparked these vendettas was a clever forgery- an edit of the public education campaign in Pakistan indented to raise awareness about child abdication. The education video begins with the kidnapping but soon after one of the hired actors gets off the bike and display a sign of warning for the viewers to protect their children. But a fake video was generated with the help of AI which went viral in India this big revel device was cut, leaving only a shocking realistic video of a child being snatched. AL technologies has made significant strides in creating the deepfake-also called the high realistic manipulated media, typically video that can make it appear as if somebody said or did something which they didn't performed. While deepfake have some legitimate use and creative use, there are also some negative aspects that raise a concern in the society.

## Deepfake

Deepfake technology breaks in the public domain in 2017 when a Reddit user used the technology to digitally produce the non- consensual porn by using the face of female celebrity. Since then the technology has spreads like the fire with the 85.047 Deepfake videos which being detected by the Deeptrace on December 2020, and the large number of non- consensual and hurtful Deepfake videos generated by the expert creators nearly doubled in every 6 Month. In the year 2019, Deeptrace estimated that over 96% of the Deepfake video circulated online which is rich in pornographic content.

Deepfake technology can be stated as the Artificial Intelligence which is probably used to generate fake images, videos and the audio recording. The term Deepfake describes both the technology and the fraudulent content and is a suitcase of deep learning and fake. Deepfake frequently alter the original source material by replacing one person with the other person. Additionally, they produce the complete original content in which a person is exhibits saying or doing something that they haven't done or said.

**Different Type of Deepfake**

Deepfake technology has processed significantly, leading to various types of Deepfake that utilize the artificial intelligence to generate a realistic but the fabricated content, here we state some main type of the Deepfake.

**1. Deepfake video**

Deepfake videos most popularly called as the synthetic video in which the likeness of one person's likeness is replaced by that of another using the AI technique. These videos involve the deep learning algorithms, specifically Generative Adversely Networks (GANs), to produce the realistic representation that in difficult to differentiate from the real one.

Deepfake mainly take the form of the AI- generated but the realistic video that helps in changing the face, creates the artificial characters or by making some edits in the existing footage. They commonly used in the movies for giving the special effects. Cyber attacker can use it maliciously by creating fake videos for blackmail, defamation, and even for the character assassination**.**

**2. Deepfake audio**

Deepfake Audio can also be highlighted as Synthetic audio that is a highly advance process which take the help of the AI to create the replica of the human voice. This technology is used to create new identities or to steal the identities of the original voice owners and spread the misinformation through the cloned audio. Similar to the Deepfake Audio and video employs advance machine learning techniques, particularly deep learning models, to crate the realistic and convincing audio clips that can mimic the target audience.

**3. Deepfake Images**

Deepfake image also stated as the synthetic image in which the person of the existing image is replaced by someone else's likeness by the help of the artificial intelligence Deepfake image is generated for the visual effect, advertising or memes etc. but on the opposite side it can also be used for the malicious act by creating the fake image to conduct misinformation campaigns or for the blackmail targets.

**4. Deepfake text**

Deepfake chats can also be stated as the edited text or the fabricated text by the help of the Artificial intelligence, heavily they are used in the chat dots as well as for the content generation. There is also a flip side of the deepfake text as they can be used to threat the people by creating fake news and content or misinformation via social media.

**5. 3D Deepfake and full body manipulation**

3D Deepfake and full body manipulation means replacing or manipulating the realistic 3D models of the people by the help of the AI or the machine learning. 3D Deepfake replace or manipulate face and body in the video and photos while full body involves editing the entire person in the three-dimension space. Such type of technologies enables hyper-realistic avatars and life like changes in the digital content.

**6. Real time Deepfake**

Real time Deepfake can be state as altering the face or voice of the person during the live video or streaming, with the use of the AI. Real time Deepfake also allows the on-the-fly changes like swapping face or modifying the face expression in the real time, as going with the darker side it also raises the privacy and misinformation concern.

**7. Synthetic Media and AI Avatars**

Synthetic Media is an AI- generated content, such as deepfake and voice synthesis, that produce the realistic digital representation.

AI Avatars are virtual representation of the people that are used in the game or interaction to mimic their appearance and behavior.AI Avatar can also be said as the digital human that mimics human movement, expression and speech pattern to provide realistic virtual interactions. In the other word AI Avatars enable you to produce high quality video content without ever picking up a camera. Furthermore, AL actors can communicate in dozens of different languages, expanding the reach of the content.

**Evolution of Deepfake**

- **Early beginning and Conceptual foundation**

The notion of altering or modifying visual media is not new, as it can be traced back to the early photograph. In the 19$^{th}$ century, these altering techniques were used to retouch or to alter the existing images, Analog method. However, the concept of using the computers to generate the fake images began to take shape in the late 20$^{th}$ century with the revolution of the computer graphic.

- **The Emergence of Machine Learning and GANs**

The rise of machine learning in the s represented the significant shift in the potential of media manipulation. Deep learning which is the subset of the machine learning, led to the revolutionary shift in how computer learned and generated data. The process was further lightening up be Lan Goodfellow and his colleague. GANs comprises of two neural networks: A generator which create a deepfake data and a discriminator that tries to distinguish between the real and the fake data, through this GANs become efficient to produce high realistic synthetic image and the video, laying the groundwork that would refer to as deepfake.

Working of GANs the working of the GANs goes with three steps i.e. first start with the generator who will generate the forged data second goes with the discriminator who will evaluate the data and the third follows the endless loop.

- **Deepfake Emergence (2017)**

The term Deepfake got popularity in 2017 when Reddit used the name "Deepfake" by posting pornographic video that layered with the face of a celebrity onto the body of the Adult film Actor by using GANs. The simplicity and the realism of the video that is created, raise the immediate concern. This was marked as the first public encounter with the deepfake, and it sparked widespread interest and the fear also talk about the potential and misuse of the technology.

- **Rapid Advancement and Accessibility**

With the running time the development and the development and the dissemination of the deepfake technology advance rapidly. It starts to appear online, allowing anyone with the computer to create convincing deepfake using relative ease. This democratization of technology resulted in the proliferation of deepfakes, all around the internet, from the harmless pranks to the maliciously application.

- **Deepfake in the Politics and Misinformation (20 18-2020)**

By the 2018 deepfake were acknowledged as a significant tool for spreading misinformation, epically in the political sphere, for e.g. a Deepfake of the former president Barake Obama, created by a filmmaker Jorden Peele and Buzzfeed, demonstrated that the deepfake has the potential to mislead the public on a large scale. As the political tension increase globally, the concern that the deepfake may be used to influence the election spread propaganda, incite violence become the serious concern.

- **The Retaliation to Deepfake**

To address the growing threat of the deepfake, government technical companies and researchers started developing strategies for detecting and minigating there impact. Tech giants like Facebook, Google and Microsoft launched initiative to develop deepfake detection tools. While the academic institution focused on developing the field of digital forensics to identify synthetic or the deepfake Media. Similarly, legislation in the several countries, including the US, begin proposing bills, particularly in the case of nonconsensual pornography and political disinformation.

- **The evolution of Deepfake Technology (2025)**

Deepfake technology evolved in the tandem with detention methods. The ongoing arms race between the deepfake creators and the detectors had resulted in the creation of the increasingly sophisticated methods for avoiding detention. Today deepfake can not only mimic visual appearance, voice, mannerism, and even personality traits, making them more convincing and difficult to identify. In recent year, the number of deepfake has doubled every six months. A projected 8 million deepfake will be shared in 2025, up from 500,000 in 2023. Europal estimated that 90% of online content may be generated synthetically by 2026 as the deepfake is spreading rapidly through social media platform, messaging apps and the video sharing platform, which blur the line between the reality and the friction. This makes it a strong tool for spreading misinformation and disinformation.

However, this period also saw significant stride in the public awareness and education about the deepfake. Media organization, educators and online platform have become more focused in education the public about the dangers of the deepfake, promoting the digital literacy is a critical tool in combating misinformation.

Deepfake with the help of the AL can create a hyper realistic synthetic media, which also give a birth to the complex issue in the digital age. It comes with a significant issue including misinformation, fraud and reputational harm, because the generator fabricates the authentic data by the aid of AI. But as every coin have two face deepfake on the other hand; provide transformative benefits in the field of entertainment, education and the creative arts by improving storytelling and personalized learning experience.

**Benefits and Threats of Deepfake**

Deepfake technology, which utilizes artificial intelligence to create hyper-realistic fake video and audio, has garnered significant attention for its potential application and implications. This technology can have the positive as well as negative impact across various sectors**.**

**Benefits of Deepfake**

Deefake, which is often considered with risks, also provide the significant benefits across a wide range of industries, all thanks to their ability to generate highly realistic synthetic media. In the entertainment industry, deepfake enhance filmmaking by enabling seamless digitals character creation and age manipulation, enriching storytelling without costly reshoots. Educational application includes personalized learning experiences that bland reality with imagination. They also hold potential in healthcare, stimulating, patient interactions for training, and in marketing, crafting hyper personalized campaigns. Harnessing these benefits, demands responsible use and support by clear regulation and ethical guideline to maximize the positive impact while minimize misuse in an evolving technological landscape.

**1. Entertainment Industry**

Enhancements of entertainments and media production the development of deepfake has enable film makers to edit image with unprecedented realism. Technology has revolutionized the entertainment industry. AI's ability to superimpose voice and facial characteristics onto previously recorded video allows for smooth performance is not present. When studios forego costly reshoot or extensive makeup in favor of editors modifying pre-recorded footage to fit new plots, production cost fall dramatically.

**2. Economical Marketing**

Deepfake improves effectiveness by reducing the marketing expenses as the traditional video advertisement are not pocket friendly and time consuming, requiring performance, location and multiple sessions. Deepfake can use to create ads using pre-existing videos or licensed digital identities, can help in increasing the effectiveness while decreasing production cost. Without filming a company can record a spokesperson and then alter their voice or appearance to appeal to different audience. Furthermore, deepfake technology reduces the production time, instead of week to day the final result is a lean flexible marketing approach that are both creative as well as cost effective businesses by producing polished, professional content as a fraction of a regular price.

**3. Tailored content**

Deepfake allows business to engage with the diverse range of customers by providing customized content business can connect with specific ethics or geographical groups, by changing the language or accent or even the appearance of speaker in their advertisements. Consider the basic campaign in which the same basic footage is used for ads starring a Mandarin speaking male in china and Spanish speaking lady in Latin America. The approach is both effective and sympathetic in providing customers with genuine representation.

**4. Immersive leaning**

Deepfake give teaching a new dimension revolutionize the educational industry teachers can instantly create multilingual content empowering students all over the world by overcoming language barriers. An AI coach who speaks French can also assist English speaking students while making adjustments in real time. Furthermore, deepfake concretize abstract ideas by stimulating situations such as debates with the history figures. Al recreation of John F Kennedy's "lost" speech for example creates a direct link to

past. It saves money because schools do not need to hire additional teachers or interpreters. Deepfake democratize information by providing high quality education without any physical resources in improvised or ruler area as a result learning became adventure rather than a case in the classroom where curiosity thrived.

**5. Reenactment of Historical Events**

Enhancements of entertainments and media production the development of deepfake has enable film makers to edit image with unprecedented realism. Technology has revolutionized the entertainment industry. AI's ability to superimpose voice and facial characteristics onto previously recorded video allows for smooth performance is not present. When studios forego costly reshoot or extensive makeup in favor of editors modifying pre-recorded footage to fit new plots, production cost fall dramatically or video exists. By using authentic course data as training data, it will able to generate data for historical events. This will be game changer for both the historians and student because it will provide visual stimulation. Student will have to opportunity to witness events such as WWII related media and speeches by historically significant figures. This will also help museums to create immersive exhibitions that will engage and pique visitor's interest. Forbs and ATM lab at CMU AI describes how he animated old photos and recreated old voice such as Salvador Dali "speaking" in his museum. Historians can transform a static archive such as old portrait, into moving, talking figures, providing a universal insight into the past.

**Threats of Deepfake**

Deepfake, powered by sophisticated AI algorithm, has emerged as a formidable challenge in the digital age. Capable of generating hyper-realistic yet fabricated audio-visual content. These technologies threaten societal trust by enabling malicious, actors, to spread misinformation, manipulate public opinion, and perpetrate fraud. From creating deceptive political propaganda to impersonating individual for financial scams, Deepfake undermine the authenticity of digital media. There potential to erode privacy, fuel cyber bullying, and damage reputation is profound, particularly when used without consent. The accessibility of deep fake took amplifies these risks, allowing even non-experts to produce convincing forgeries.

**1. Identity theft**

Identity theft or impersonation means unauthorized access to the personal information of any individual and using personal information to commit fraudulent activities. The deepfake technology gives superpower to cyber criminals to impersonate individual with hyper-realism by replicating the individual's persona. This is accomplished by using data available on social media, which is used to train data, resulting in synthetic media with an unreal resemblance to the targeted victim.

**2. Authentication System**

Authentication system, deepfake can also replicate biometric data such as audio or video authentication, which is a concern of biometric security, which can be the threat for the society. In 2019, a case was witnessed where the Deepfake was used to mimic the voice of the Company Director, and convinced the manager of Hong Kong Bank to authorize a transaction worth of $35 million as part of what at first sight seemed like a legitimate acquisition deal. The attack combined forged email, document and deepfake audio. Attackers were able to take out $ 4000,000 before getting deducted. They showed potential misuse of deepfake technology.

**3. Erosion in trust in digital communication**

One of the primary advantages of the internet is the ability to share information over long distance in a very short period of time, digital communication in one aspect of cyber security. Deepfake can be used to disseminate misinformation, undermine institution or sway public opinion. A deepfake video or image making false claims could go viral causing panic and disrupting stock market and diplomatic relations.

In 2024 a scammer impersonating billionaire Elon Musk circulating a deepfake video in which Musk can be heard saying, "here's a surprise for everyone I will be doing a give away at Elon4u.com for one week stating on December 13" scamming people in the "giveaway." Many people trusted the scam and lost their hard earn money

**4. Corporate espionage**

Corporate espionage is made possible by the use of technology. Deepfake technology enables cybercrime to impersonate a managerial person during telephonic or video conferencing, in which he can ask for trade secret or other important information that is not publically available.

In the news report of the Wall Street Journal, it was confirmed that in 2019, a CEO of a UK- based energy company was defrauded of $243,000 when he gets the phone call from CFO of the firm's German parent company, and he asked to transfer the amount to Hungarian suppliers. The voice of the German CFO was generated by the help of the Deepfake, and believing it to be an order of the boss; the CEO transferred the money to the scammer.

**5. Reputation Threat**

Deepfake creates media in which people are seen saying they never said; this undermines the victim's confidence and trust, making it difficult to remove the satin from the reputation. In a deepfake video of Belgium's Prime Minister, Sophie Wilmes, was seen linking climate change with the COVID -19. This resulted in challenging the credibility of Sophie Wilmes, damaging her reputation ambits the sensitive political period.

**6. Electoral Disinformation**

Any Democratic country, as any individual organization, or even another country impedes this process by installing distrust in leaders, through the dissemination of false information. Deepfake have a several emotional and psychological impact on the victim, making them useful tool for disrupting fair elections. Impersonating political figure and spreading false information about any leader will manipulate voter's perceptions of electoral candidates, thereby undermining citizen, free will in the targeted country.

**7. Effect on judicial system**

There is next to no chance to have a direct effect on the judicial system but as judges are also the human being and they also get affected by the societal perception. Deepfake

can be used to create evidence that is likely to be discarded if its origin is unknown, or there is any suspicion that it has been tampered with. However, it will not only cause a delay in the process, but it will also have an impact on public perception. Defendant, on the other hand, can use it to call into questions, the legitimacy of an original audio, image or video created by Deepfake, liar's dividend.

**Indian Regulation Framework on Deepfake**

**1. Constitution of India**

Freedom of speech and expression Article 19 of the Indian Constitution is a cornerstone fundamental right enshrined in part III of the Constitution, and it guarantees citizen, certain freedom necessary for a democratic society. It strikes a balance between individual liberty and societal needs, granting rights while allowing the states to impose reasonable restrictions.

Article 19 (1), list six freedom is guaranteed to all citizens, while Article 19 clause 2–6, specify the conditions under which the state may impose reasonable restrictions on these freedoms, ensuring that they do not jeopardize public interest or national security. Article 19 (1) (a) mentions about freedom of speech and expression, which allows the Indian citizen to express their thoughts, opinion, and believe in any medium, including work, writing, painting, and pictures. This includes press freedom, and in the modern era, digital expression, such as social media.

In the case of Shreya Singhal versus Union of India, the Supreme Court upheld the law's broad scope, which includes online speech. Thus, a blanket ban on deepfake generated media cannot be imposed because it is protected by article 19 (1) (a) as part of free speech and expression. Article 19 (1) (a) grants freedom, while article 19 (2) impose reasonable restrictions on ground such as public order, decency, morality, defamation, or state security. This balance allows the regulation of harmful content.

Article 19 prohibits the deepfake that spread misinformation and threaten public order or defamation. The state could not enforce the clause prohibiting malicious Deepfake on these grounds while allowing legitimate expression such as satire. The court may uphold such restrictions if they are proportionate, as seeing in the Shreya Singhal case, a landmark decision on the right of free speech and its reasonable limitations.

**Article 21 Right to life and personal Liberty**

Protection of life and individual liberty, Article 21 of the Constitution of India states, "No person shall be deprived of his life or personal liberty, except in accordance with the procedure established by law."

As a "reservoir of right", Article 21 adapt to societal changes, serving as a safeguard against emerging threats such as deepfake its play with other rights, broadens its proactive reach. For example, the deepfake- generated media that falsifies, a person 's voice or video, would Jeopardize privacy, dignity, and mental health, all of such have been interpreted under article 21.

A violation of privacy occurs when a fake video depicts an individual in a fabricated, explicit scene, infringing on their informational and physical privacy, under Article 21, victim can petition the court for an injunction to stop distribution as well as damages for emotional harm. The landmark decision in the KS Puttaswamy versus Union of India established that privacy is an inherent part of article 21, which includes information privacy, body autonomy, and protection from surveillance or misuse of personal data

Dignity is an essential component of Article 21, which protects individual from humiliation or degradation, Deepfake can diminish someone's dignity by portraying them in a compromising or false context. In the landmark case of the Francis Coralie Mullin versus the Union territory of Delhi, it was determined that the meaning of life extends beyond animal existence to include dignity and the right to live with human worth. A deep fake defaming, a public figure in a scandalous manner would be beneath their dignity. The court would order platforms to remove such content, citing Article 21 and penalizing the creators.

The right to livelihood is derived from Article 21 of the landmark case of Olga Tellis versus Bombay Municipal Corporation, which protects economic stability based on reputation or profession. A Deepfake by a CEO, which result in a first statement, could cause a stock market, clash, threatening job, affected parties may seek a judicial remedy to halt circulation and recover compensation.

Fundamental Duties Article 51A outlines 11 duties for citizen. The 42nd Constitutional Amendment Act of 1976 added 10 duties that has not been part of constitution since its inception. The 11$^{th}$ was added in 2002 with the 86th Constitutional Amendment Act. Fundamental duties have enormous persuasive power. In the case of A.I.I.M.S student union versus A.I.I.M.S and others, the Supreme Court state that in case of doubt or choice people's wishes as manifested through Article 51A, can serve as a serve guide for constituting or moulding the relief to be given by the court, "court must use constitutional enactment of fundamental duties to keep track of state actions that deviates from constitutional value".

Article 51A(e), which imposes a duty on citizens to promote harmony and renounce practices that degrade, women's dignity, and article 51A (h)which encourages citizen to cultivate a scientific temptations and spirit of inquiry. Deepfake, harming women would violate the spirit of Article 51A (e). Article 51A (h) encourages ethical AI use by promoting educational campaigns or regulation to prevent misuse and indirectly cultivating a culture against human deepfake.

**2. Digital Personal Data Protection Act, (2023)**

Digital personal data protection act 2023, enacted on August 11, 2023 aims to protect personal data in the digital realm while balancing the need for lawful data processing. The DPDP Act provides a framework to address the growing threat of the technology, which use artificial intelligence to create hyper – realistic, but fabricated media that threatens privacy, misinformation, and public trust. The DPDP act will replace Data protection law.

The DPDP Act will supersede data protection law under the Information Technology Act and the Information Technology (reasonable security practice and procedure and sensitive personal Data or information) Rule 2011("SPDI Rules") the SPDI regulation only require entities to obtain consent when collecting "sensitive personal data" which is a comprehensive list. Under the DPDP Act, entities are required to obtain consent for all personal data collection and proceeds.

Deepfake and manipulation of personal data, such as people's, likeness, voice, and behaviors often without their consent, to create misleading content. This can result in

privacy violation, reputational harm, financial fraud, and social rest. While the DPDP act does not specifically mention deepfake, its provisions or data protection, consent, and accountability can be interpreted and used to effectively address this issue. The Act establishes a multilayered approach for protecting against the use of personal data that could be used to create the deepfake, which are as follows.

Section 4, 5, 6 and 7provide prevention measures and ensuring the personal data cannot be used for the deepfake creation without the consent of the individual whose the deepfake is being created, this should be deter as unauthorized use of personal data for ii Measures for data protection under section 8, 9, 11 and 13 to prevent misuse and ensure data integrity, with a focus on platforms that sell users data or allow the creation of Deepfake (3) Section 10, 33 and 37 contain measures to deter the misuse of personal data for the creation of Deepfake ,including penalties, and potential access restrictions that discourage both creators and disseminator.

Section 3 of the DPTP Act defines the scope and the applicability of the act. The Act shall apply to the processing of digital personal data within or outside India. (If such processing is related to the activity of processing data for the provision of goods and services of data principles within India) Deepfake typically involves the manipulation of personal data, such as images, voices, or biometric to create fabricated content. If a fake is created or distributed by an entity that provides services in India, such as social media platforms, it is subject to jurisdiction of this Act.

The act also has extraterritorial jurisdiction which ensures that foreign platform hosting their services in India. Do not use personal data to create content targeting India users, and if they do, they can be held accountable.

### 3. Indian Copy Right Act, Of 1975

The deepfake powered by artificial intelligence generate high realistic, but synthetic media, raising Legal concern about their use. Despite the lack of specific provision for this technology, India's Copyright Act, serve as an important mechanism for regulating the deepfake space when it comes to copyright, content or performer's right.

According to section 57, infringement occurs when someone performs any act for the copyright owner, such as copyright or adapting a work, without permission, unless the act expressively states otherwise. This provision covers deepfake that incorporate protected content without consent. In a scam, using a deepfake audio to replicate a musician's, copyright is a violation of article 57.

Section 52 includes exceptions, such as fair use for private use, criticism, review or reporting. These exceptions are specific and do not broadly cover deepfake – related activities, thus, the fair use exception cannot be invoked by anyone creating synthetic media, malicious deepfake, such as those use for blackmail or misinformation and legally accountable due to their intent and impact.

### 4. The Prevention of Child from Sexual Offence Act, 2012 [32]

The Prevention of Children from Sexual Offence Act of 2012, (POCSO) was enacted to protect children, one of the societies, most vulnerable group and the future of any country, from all forms of sexual violence. The act imposes harsh penalties for any sexual abuse, committed against children under the age of 18. Chapter III of the Act makes it illegal to use children for pornographic purpose, as well as to store pornographic materials involving a child. Although POCSO does not explicitly mentions the deepfake, the sections broad phrasing can address the misuse of the deepfake technology by children.

Section 13 of POCSO defines the offence of using a child for any form of media for pornographic purpose, whether for personal use or distribution.

Section 15 of POCSO defines and penalizes the act of storing pornographic material involving a child. Any person who keeps pornographic material involving children and fails to destroy, delete or report it to the authorities, the person who store such media with the intention of sharing a transmitting it face up to three years of imprisonment, a fine or both.

### 1. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [33]

Information technology, intermediary guidelines and digital media ethics code rules of 2021D, Deepak, which use Advance AI techniques like generator adverse network, have become a major concern in India as evident by incident like 2023, Deepak of actress Rashmika Mandanna and manipulated political content during elections. The IT rule 2021, which was announced on February 25, 2021, to regulate intermediary's entities that facilitates the storage, transmission and access of third-party content by imposing due diligence obligations and accountability Mechanism. This section examines the specific provision of the IT rule 2021 that deals with deepfake, explains how they regulate such content and evaluate their practical impact in Indian legal and technological landscape.

Rule 3(1)(b) prohibits harmful content. Rule 3(1)(b) requires intermediaries to prohibit users from posting, display, upholding, modifying, publish, transmitting, storing, updating, or sharing content that is obscene, pornographic, or invasive of privacy threatening, security, public order, friendly relation with foreign states or impersonate, other persons or promote false information, then it comes under the ambit of 3(1)(b).

### 2. Information Technology Act

Information technology Act, (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021, deepfake, which use Advance AI techniques like Generative Adversarial Network, have become a major concern in India, as evident by incident like 2023, deepfake of actress Rashmika Mandanna and manipulated political content during elections. The IT Rule 2021, which was announced on February 25, 2021, seeks to regulate intermediary's entities that facilitate the storage, transmission and access of third-party content by imposing diligence obligations and accountability Mechanism. This section examines the specific provision of the IT Rule 2021 that deals with deepfake, explains how they regulate such content, and evaluate their practical impactions in India's legal and technological landscape. The Information technology Act of 2000 [34] was enacted to recognise electronic records and accelerate the growth of e-commerce in the new age of information exchange. The information technology Amendment Act 2008 [35] is one of the most significant changes to the IT Act 2000. When India entered the internet era, the benefit and drawbacks of the internet become clear,

and Act of 2008 was enacted to strengthen India's regulatory framework covering cyber security. It was a Keen- Jerk reaction to the terrorist attack of 26/7.

If we take a broad, interpretation of section 66C, we can use it to punish people who use the deepfake technology to steal identity. The deepfake technology makes use of distinctive identification features, such as the creator's face, voice, and other distinguishing character. It is important to note that the creation of the deepfake media does not continue identity theft unless it is indented for dishonest or purpose.

Section 66D makes provisions for criminalizing cheating by personating and using computer resources. It states that "whoever, by means of any communications device or computer resources, cheats by personation shall be punished with impressment of either description for a term which may extend to 3 years and shall also be liable to a fine of up to 1,00,000 rupees.

Section 66E makes provision for criminalizing invasion of privacy. It states that "whoever, intentionally or knowingly, capture, publishes or transmit the image of a private area of any person without his consent, under circumstances, violating that person's privacy shall be punished with imprisonment for up to three years or fine, not exceeding two lakh rupees, or both "This right has been as fundamental right, and it's violation is punishable under this section."

Section 67, criminalizes the, the publication or transmission of obscene material in electronic form. This section addresses the act of publishing, transmitting or causing to be published any electronic materials that is lascivious (lustful), appeals to prurient in interest (a healthy curiosity about sex), or has the potential to deprave and corrupt, those who come into contact with it. It applies to the content deemed obscene under the Indian legal standards; emphasize the effect on viewers rather than the internet itself.

Section 67A of the IT act specifies the penalties that publishing or transmitting materials containing sexually explicit content. This section prohibits material that consist sexually explicit act or conduct including graphic descriptions or sexual activities. It is narrow and more sensitive than section 67, emphasizing explicitness and lasciviousness.

Section 67B of the IT act, punishes the publication and transmission of material depicting children engaging and sexually explicit activities. This section provides special protection to children, who are the future of any nation form the publication and transmission of media depicting them in a sexually explicit activity. This section specifically addresses media depictions children under the age of 18 engaging sexually explicit act or conduct, including the creation collection, browsing, downloading, or distribution of such material.

Section 79 of the IT Act, establishes a "safe harbor" of the intermediaries, such as YouTube, Facebook, X, and other hosting services, exempting, them from liability for users generated content, if certain conditions and met such as neutrality, no modification and the removal of illegal content upon receipt of a government order. This section intersects with the Copyright Act and explains the case of Myspace Inc versus Super Cassettes Industry Ltd. decided by the honorable Delhi High Court in 2016, a music company claims copyright infringement for the songs uploaded by the user.

### 3. Bhatiya Nyaya Sanhita

Deepfake technology can generate hyper realistic fabricated audio, video and images. This type of fraud has emerged as a serious threat to the People's dignity, financial security and societal stability. Despite the fact that it does not explicitly mention Deepfake the BNS is a fundamental regal tool for combating this threat. The existing legal framework is being used to combat the threat of deepfake. The following is a detailed explanation of how specific BNS sections can be used to combat deepfake related offences, grouping similar provisions for clarity and demonstrating the specific application.

**Cheating**

Cheating is defined as the act of fraudulently deceiving another person in order to induce them to deliver property, consent to action, or cause harm to their body, mind, reputation or property. Deepfake demonstrate this by impersonating individuals in order to trick others into financial transactions or obtained sensitive information. If such kind of the activity happens then victim may file a case under section 318(1) of BNS if deepfake media leads to fraudulent inducement. The prosecution must prove intent to deceive as well as the resulting harm, which may include financial loss or reputational damage.

**Cheating by Personation**

Cheating by Personation occurs when one person deceives another by pretending to be someone else or misrepresent another person's identity in order to gain an advantage or cause harm. This definition emphasizes impersonation as a key method of deception, setting it apart from general chatting. Deepfake demonstrate this practice by producing realistic audio, video or images that mimic a person 's voice, face and behavior.

**Offence related to fraud and deception**

Deepfake can generate hyper realistic media that can be used to impersonate people in positions of authority in order to force others to make decision based on their advice or orders. As a result, individual can use deepfake to commit financial fraud or deceive others through impersonation. To combat the threat of fraud and deception via deepfake, BNS provides the following section.

**Forgery**

Forgery is defined as the creation or alteration of false document or electronic record with fraudulent intent in order to cause harm or injury to individuals to cause harm or injury to individual or public, support claims, induce property transfer, or facilitate fraud. The information Technology Act of 2000 [34] expended, this definition to include "false electronic record, making it applicable in digital context such as the deepfake. Key components of forgery include creating fall, document or electronic record, intend to cause harm or injury, support for a claim or title inducing someone to part with property or enter into a contact Intend to commit fraud Deepfake falls under the category of "false electronic record", as they are designed to misrepresent reality with malicious intent.

**Forgery for the purpose of causing reputational harm**

Forgery for the purpose of causing reputational harm is a specific offence defined as the act of forging with the intent of harm someone's reputation or knowing that the forged

document or electronic record will be used for that purpose. This offence carries a penalty of up to 3 years in prison and fine. The key element of this offence is forgery is the creation or alteration of a document or electronic record intended or knowingly. The perpetrator intent to harm the reputation or is aware of the possibility of harm. Reputational harm the act is directed at an individual's, social standard credibility or public image.

This section is particularly relevant in the context of deepfake, which can be used to defame or humiliate individuals. For instance, deepfake videos designed to tarnish someone's image, such as incident involving actress Rashmika Mandanna exemplify, the malicious use of synthetic media for a reputational damage. The law focuses on the act, of forging contact rather than merely its dissemination, making it suitable for prosecuting case like non-conceptual deepfake pornography of fabricated scandals. While the provision is effective, its success hinges or proving intent and addressing anonymity challenges often require forensic evidences. This section complements existing defamation laws and is integral to India's legal framework addressing deepfake related reputational attack.

**Words, gestures, or acts intended to insult the modesty of a woman**

The provision prohibiting word gesture or act intended to insult a woman's modesty is a gender specific law defined to protect women's dignity and privacy punishable by the three years imprisonment and fine. Introduced in the IPC 1860 and later amended it and increase the punishment from 1 year to 3 years, it reflects Indian's commencement to protecting women's honor in a particular society. The intention to insult, the nature of the act, and the targeting of women are all important consideration.

The provision covers deepfake, particularly non-consensual pornography which can degrade a women's modesty. A notable case involved actress Rashmika Mandanna, whose face was superimposed on another women's body in a deepfake video, returning in public humiliation. The Delhi Police field a FIR against the perpetrator for and privacy violation, emphasizing the legal consequences of such action.

**Defamations**

Section 356(1) of BNS outlines the elements required for the offence of defamation as follows communication in the act of making or publishing statement, using spoken words, written words, sign or visual representation. Imputation- the communication must include an imputation about an individual. Intent of knowledge- the individual must either intent to harm the person 's reputation or know or have the reason to believe that they will do so. In summary defamation, when someone make positive statement about another person with the intent to harm representation or knowing that such statement harm that person standing.

Deepfake which are manipulated or generated medium that falsely portray individual in dim change situations can be considered under section 356 of BNS. The term used in the section such as representation and words intend to be read. Refer the digital content which makes them applicable to deep fake when a deep fake is create or share with the intent or knowledge that it will harm a person reputation. It is considered definition or characteristics of correspondence to sign a representation and sharing such content online with the requirement for publication.

**Voyeurism**

Following by the Nirbhaya case is the criminal law (amendment) Act of 2013, added voyeurism to the Indian Penal Code in order to combat sexual offences against women, other than physical assault. Justice Verma Committee formed in response in that incident recommended strong privacy law which resulted in the inclusion of section 354C in the IPC. The section emphasizes individual dignity and autonomy, which is consistent with the current Justice Principal and reflected in the BNS.

Section 77 of BNS takes a genderneutral approach to voyeurism allowing both men and women to be offenders, unlike IPC which states that only "any man" can commit such an offence. Section 77 key elements include action like, watching a woman perform a private act, capturing her image in such situation, and disseminating that image. Private act, as defined in the section include behavior such as exposing genitals (even if they are covered by underwear), using the restroom are engaging in sexual acts that are not typically performed in public. These acts occur in areas where people have a reasonable expectation of privacy.

**Criminal intimidation**

Section 352 of BNS is a part of chapter XIX which deals with public order offences like criminal intimidation and defamation. This section criminalizes deliberate insult intended to elite reactions that disrupt public order or leads to additional offence. It modernizes and replaces section 504 of IPC updating the language to reflect current legal standard while preventing the core principal. The primary goal of the provision is Social harmony in the India's diverse society, by discouraging provocation behavior that may incite violence or disorders.

Synthetically generated media, such as deepfake and audio recording, can be used for extortion. For example, a deepfake video may depeict a victim in vulnerable station threatening exposure unless ransom is paid, installing fear of reputational harm. Similarly, a phony audio recording of a victim's loved ones for assistance can exploit emotional vulnerability, promoting the victim to pay them alleged amount. These tactics use realistic threats to coerce people into delivering money or valuable.

Section 152 of BNS specifies the requirements of the offences of endangering India's sovereignty, unity and integrity. It states that anyone who intentionally incites secession, armed rebellious activities are promotes separatist sentiments, is committed a crime such as actions can result in severe penalty such as life imprisonment, or a seven-year prison sentence as well as a potential fine.

Deepfake can be created convincing false narratives, are punishable under section 152 if they are spared to disrupt social harmony or national interest, for example, a deepfake depicting a public figure, inciting violence prosecuted under the section if intented to disrupt its proven. However, its broad language makes no specific mention of Deepfake technology for regulating precreation of non-malicious users.

**4. Cyber security framework of India-**

**a. The Indian Computer Emergency Response Team (CERT – in).**

The Ministry of Electronics and information technology, MeitY overseas the Indian computer Emergency Response Team (CERT) its functions include serving as a point of contact for reporting local problems, assisting organization and the general computing community in preventing computer, security breaches, issuing guidelines and advisory vulnerability analysis and response, profiling attacks, conducting training and so on. On November 27, 2024, the CERT – In issued and advisory CIAD – 2024–00060, title "Deepfake- Threats and countermeasures" to help organization and individuals educate themselves and prepare for the deepfake threats. The advisory informed people about the deepfake technology and scam that can result from using hyper-realistic synthetic media, such as financial fraud, disinformation, social engineering, non-consensual, explicit content, or rising sophistication.

**b. Indian Cybercrime Coordination Center (I4C) Schemes**

With the rise of cyber crime in India, including hacking, online fraud, and entity theft, and crime against vulnerable group such as women and children, the 14C scheme was approved on October 2018 with a budget of ₹415.86, 00, 00,000 it was formally established on January 10, 2020, by the Union Home Minister Amit Shah in Delhi making a watershed movement in India's fight against cyber crime. 14C is a comprehensive initiative launched by the Indian government to combat cyber crime in coordinate and effective manner. 14C, established by the Ministry of Home Affairs serves as a central hub for coordinating efforts among law enforcement agency, industry, academic, and other stakeholders.

**5. Indecent Representation of Women (Prohibition) Act, of 1986 [47, 50]**

The Indecent Representation of Women Prohibition Act of 1986 [47, 50], IRWA was passed to prevent incident and derogatory representation of women in various media. With the rise of deepfake technology, artificial intelligence generates synthetic, but hyper-realistic media that is frequently erotic in nature. It prohibits objectifying or degrading women.

If a deepfake is embedded in an online advertisement are widely distributed for attention, Section 3 can target those who created or distributed it. Even if not strictly an "advertisement" interpretation could broaden it's a scope to include public – facial digital content. For example, a defect video mocking woman in a derogatory way and uploaded to a monetized YouTube channel may trigger section 3 liability for the uploaded.

Section 4, specifically defines "film, photographs and representation" as regulated media, which includes deepfake video and images. Deepfake, which are digitally, manipulated visuals, or audiovisual content, fall into these categories, the term "representation" is particularly broad, and encompassing, any form of deputation, real, and fabricated, that defects women inappropriately.

**Suggestions and recommendation**

**Enact specific deepfake legislation and strengthen the existing one**

Government should develop and enact those law that specifically addresses the creation distribution, and use of deepfake these laws should define deepfake clearly and establish the patently for malicious use, particularly in case of misinformation, harassment or fraud. With that the government should also revise current privacy and defamation laws to include protection against deepfake technology can provide individual with legal resources. This includes ensuring that individuals have control over the use of their likeness and voice.

**Encourage transparency in AI development**

Promoting transparency in the development of AI technologies can help to mitigate the risk associated with deepfake. This includes encouraging developers to disclose the use of deepfake technology in content creation and providing user with information about the authenticity of media.

**Launch educational initiative**

Government should initiate public awareness campaigns aimed at educating citizens about deepfake. This includes inform the about the potential danger of the deepfake, how to identify them and the importance of verifying information before sharing.

**Promote media literacy program**

Incorporating media literacy into educational curricular can empower individuals to critically evaluate the information that encounter online. Teaching skills related to identifying, misinformation and understanding the implementation of deepfake essential.

**Educate yourself about the Deepfake**

Understanding what deepfake are, how they are created and their potential implementation is the first step in combating misinformation. Familiarize yourself with technology, and its uses to better recognize the deepfake content.

**Use fact, checking tools**

Use fact, checking websites and tools designed to identify deepfake and misinformation platform like fact check organization, snopes, and other can help verify the authenticity of content.

**Think before you share**

Consider the potential impact of sharing content before posting it on social media or forwarding it to other. If you have doubt about the authenticity, refrain from sharing it until you can confirm its validity.

**Report deepfake Content**

If you encounter deepfake content which is misleading or harmful, reported the platform where it was found. Most social media site have mechanism for reporting misinformation or harmful content.

**Conclusion**

Deepfake technology embodies are dual edge sword, offering both remarkable opportunities and significant challenges. On the positive side, it enhances creativity and entertainment, foster innovative, educational method and promotes accessibility for diverse audience. This application highlights the potential of deepfake to enrich our media landscape and provide unique experiences. The negative

implications cannot be overlooked. The potential for misinformation privacy violation, erosion of trust in media, and security threats, raises serious ethical concern. As deepfake technology continue to evolve, it is crucial to implement, safeguard and foster discussion around responsible use to mitigate its risk.

The legal implication of deepfake technology presents significant challenges that current law struggle to address efficiently. As deepfake become increasingly sophisticated and prevalent, the existing legal framework often fall short in providing adequate protection against its misuse. Moreover, the rapid evolution of deepfake technology outpaces legislative process, making it difficult for lawmakers to keep up with the necessary regulation. While some jurisdiction has begun to introduce a specific law, targeting deepfake, these efforts are inconsistent and very widely across regions, leading to a patchwork of regulations that can be inefficient in addressing the global nature of the problem. To enhance the efficiency of law regarding deepfake technology, a multi-faceted approach is required. This include developing comprehensive legislation that specifically address the nuance of deepfake, strengthening, existing privacy and defamation, law, and fostering collaboration between government, tech companies, and legal expert. While concluding the current law provides a foundation for addressing some aspects of deepfake technology, they are insufficient in their current form. A protective and unified legal response is essential to mitigate the risk associated with deepfake, protect individual's right and uphold the integrity of information in the digital age.

**References**


1. NYU Tandon School of Engineering. NYU researchers develop new real-time deepfake detection method. IEEE Spectrum. Available at, 2025. https://spectrum.ieee.org/real-time-deepfakes.
2. Tully, M. What is an AI avatar Colossyan.com Available at, 2025 https://www.colossyan.com/posts/what-is-an-ai-avatar?
3. Regan G. A brief history of deepfakes. Realitydefender.com. Available at, 2025. https://www.realitydefender.com/insights/history-of-deepfakes.
4. Kapoor A. Study of deepfakes and misinformation. SSRN, 2024. Available at, https://papers.ssrn.com/sol3/papers.cfm?abstractid = 5021575.
5. GeeksforGeeks. Generative adversarial network GAN. GeeksforGeeks, 2025. Available at. https://www.geeksforgeeks.org/deep-learning/generative-adversarial-network-gan/.
6. Cyble. What is a deepfake. How to spot? Different types. Cyble.com, 2025. Available at. https://cyble.com/knowledge-hub/what-are-deepfake
7. NYU Tandon School of Engineering. NYU researchers develop new real-time deepfake detection method. IEEE Spectrum, 2025. Available at. https://spectrum.ieee.org/real-time-deepfakes.
8. Kapoor A. Study of deepfakes and misinformation. SSRN, 2024. Available at. https://papers.ssrn.com/sol3/papers.cfm?abstractid = 5021575.
9. Allyn B. Where are the deepfakes in this presidential election? NPR, 2020. Available at. https://www.npr.org/2020/10/01/918223033/where-are-the-deepfakes-in-this-presidential-election.
10. NYU Tandon School of Engineering. NYU researchers develop new real-time deepfake detection method. IEEE Spectrum, 2025. Available at. https://spectrum.ieee.org/real-time-deepfakes.
11. Tully M. What is an AI avatar Colossyan.com, 2025? Available at. https://www.colossyan.com/posts/what-is-an-ai-avatar
12. Regan G. A brief history of deepfakes. Realitydefender.com, 2025. Available at. https://www.realitydefender.com/insights/history-of-deepfakes.
13. ZeroThreat, Deepfake attacks, AI-generated phishing statistics. Zerothreat.ai, 2025. Available at. https://zerothreat.ai/blog/deepfake-and-ai-phishing-statistics.
14. Lalla V, Mitrani A, *et al*. Artificial intelligence Deepfakes in the entertainment industry. WIPO Magazine, 2025. Available at. https://www.wipo.int/web/wipo-magazine/articles/artificial-intelligencedeepfakes-in-the-entertainment-industry-42620.
15. Kalmykov M. Positive applications for deepfake technology. DataArt Blog, 2025. Available at. https://www.dataart.com/blog/positive-applications-for-deepfake-technology-by-max-kalmykov. Last visited on August 07, 2025. Milenkovi A. The positive impact of deepfakes. Bluegrid.io, 2025. Available at: https://bluegrid.io/blog/the-positive-impact-of-deepfakes/.
16. BDO Singapore. Deepfakes. The dark side of AI entertainment. BDO Insights, 2025. Available at: https://www.bdo.ae/en-gb/insights/deepfakes-the-dark-side-of-ai-entertainment.
17. Damiani J. A voice deepfake was used to scam a CEO out of $243,000. Forbes, 2019. Available at: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-aceo-out-of-243000/.
18. Marr B. The dark side of AI. How deepfakes and disinformation are becoming a billiondollar business risk. Bernardmarr.com, 2025. Available at: https://bernardmarr.com/the-dark-side-of-ai-howdeepfakes-and-disinformation-are-becoming-a-billion-dollar-business-risk/. (Last visited on August 08, 2025). [4] [2015] 5 S.C.R. 963
19. Kumar S. The right to privacy in India. A critical analysis of Article 21. Journal of Social Sciences,2023:14:39. Available at: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2245context=jss.
20. (2019) 1 SCC 1.
21. 1981 AIR 746.
22. (1985) 2 BOM CR 434.
23. 2001 AIR SCW 3143.
24. The Digital Personal Data Protection Act, (Act 22 of 2023). India Code, 2023. Available at: https://www.indiacode.nic.in/handle/123456789/16867?locale=en.
25. Sahu A, Das A. A comprehensive analysis of the Digital Personal Data Protection Act, 2023 in India. International Journal of Law and Contemporary World, 2023:3(2):84. DOI: 10.54934/ijlcw. v3i2.84.
26. Section 3: Application of the Digital Personal Data Protection Act (DPDP). Apni Law. Available at: https://www.apnilaw.com/bare-act/dpdp/section-3-digital-personal-data-protection-act-dpdpapplication-of-act/.

27. The Copyright Act, 1957 (Act 14 of 1957). India Code.Available at: https://www.indiacode.nic.in/handle/123456789/1367?locale=en.
28. Id., at s. 57.
29. Id., at s. 52.
30. The Prevention of Children from Sexual Offences Act, 2012 (Act 32 of 2012). India Code. Available at: https://www.indiacode.nic.in/handle/123456789/2078?locale=en.
31. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. India Code. Available at: https://www.indiacode.nic.in/handle/123456789/15981?locale=en.
32. Id., at r. 3(1)(b). [3] The Information Technology Act, 2000, Act 21 of 2000. India Code. Available at: https://www.indiacode.nic.in/handle/123456789/1999?locale=en.
33. Information Technology (Amendment) Act, An Overview. Manupatra, 2008.Available at: https://articles.manupatra.com/article-details/Information-Technology-amendment-Act-2008-AnOverview.
34. Id., at s. 66D.
35. Id., at s. 2(k).
36. Id., at s. 67.
37. Id., at s. 67B.
38. Id., at s. 319(1).
39. Id., at s. 336(1).
40. Id., at s. 336(4)
41. Id., at s. 318(1).
42. Rashmika Mandanna Deepfake Case: Main Accused Arrested by Delhi Police. The Times of India. Available at: https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/rashmika-mandannadeepfake-case-main-accused-arrested-by-delhi-police/articleshow/107009990.cms.
43. Gender Justice in India. How BNS, Advances Beyond IPC to Ensure Equality and Protection. Legitimate India, 2023. Available at: https://legitimateindia.com/gender-justice-in-india-how-bns-2023-advances-beyond-ipcto-ensure-equality-and-protection/. 236 DLT 478 (DB).
44. Bharatiya Nyaya Sanhita, (Act 45 of 2023). India Code, 2023. Available at: https://www.indiacode.nic.in/handle/123456789/16868?locale=en.
45. Indecent Representation of Women (Prohibition) Act, 1986 (Act 60 of 1986). India Code. Available at: https://www.indiacode.nic.in/handle/123456789/1768?locale=en.
46. The Impact of Deepfake Technology, Legal Risks and Regulatory Solutions. Metalegal.in. Available at: https://www.metalegal.in/post/the-impact-of-deepfake-technology-legal-risks-and-regulatory-solutions.
47. Section 299. Bharatiya Nyaya Sanhita, 2023. Marriagesolution.in. Available at: https://marriagesolution.in/bns_section/299-bns/.
48. Indecent Representation of Women (Prohibition) Act, 1986 (Act 60 of 1986). Available at: https://www.indiacode.nic.in/handle/123456789/1768?locale=en.
49. The Impact of Deepfake Technology: Legal Risks and Regulatory Solutions. Available at: https://www.metalegal.in/post/the-impact-of-deepfake-technology-legal-risks-and-regulatory-solutions.
50. Id., at s. 79.