Assessing the Impact of Artificial Intelligence on Social Media Dynamics: Prospects and Challenges

- **Dr Ankita Kumar Gupta*** **& Ms. Arsheya Chaudhry****

Abstract

The branch of computer science known as artificial intelligence studies how well a machine can replicate human intelligence. It could assist in addressing some of the most difficult socioeconomic issues faced around the globe today and could do wonders. These days, social media also referred to as social networking consists of YouTube, Facebook, Instagram, Pinterest, Twitter etc. AI is essential to the operation of today's social networks. AI is being used in social media in ways that have never been seen before, and it is rapidly changing the platform. In the recent few years, social networking site usage among Indian internet users has increased dramatically, especially among younger generations. Additionally, the use of AI by social media has presented various difficulties for the Indian law enforcement agencies. Therefore, comprehending the application of artificial intelligence in social media and its consequences is crucial. With the right knowledge of artificial intelligence and social media, including its advantages and disadvantages, the Indian legal system can use the potential of these technologies to address contemporary issues. Given the misuse of social media, content monitoring has become essential. The paper presents SWOT analysis of the use of AI in social media trying to answer whether AI and social media are bone or bane.

Keywords: Artificial Intelligence, Social Media, Deepfake, Legal Reforms.

I. Introduction

Artificial intelligence (AI) is a technology that imitates human behaviour and gives gadgets intelligence. It is distinct from other recently developed technologies since it can alter human nature, Al is regarded as transformative technology. Nevertheless, there hasn't been a consensus definition of Al up until now, it is a ubiquitous technology that has impacted our daily existence.[1] The cognitive science of Artificial Intelligence studies intelligent machines that can carry out tasks that were

* Assistant Professor (Senior Grade), Vivekananda School of Law and Legal Studies, Vivekananda Institute of Professional Studies-TC, New Delhi, Email: ankita.gupta@vips.edu

** Perusing LLM in IPR and Technology Laws, O. P. Jindal Global University, Sonipat, Haryana. Email: 24jgls-achaudhry@jgu.edu.in

[1] Chemmalar S, 'Artificial Intelligence and Legal Implications: An Overview' (2018) 14 National Law School Journal <https://repository.nls.ac.in/nlsj/vol14/iss1/14>.

previously solely done by humans. Its primary focus is on using computers to perform activities that depends on cognitive, perceptual, reasoning, and comprehending skills. Individual behaviours, tastes, opinions, and interests can be leveraged by AI systems through training to personalise experiences. Machines can be trained to mimic human behaviour. They can provide them the capacity to hear, see, move, write, and speak. AI is far more adept than humans at picking up these habits. Numerous sectors are using AI technologies to automate and improve the efficiency of a range of jobs.[2]

II. Application Of AI in Social Media

A variety of web-based and mobile systems that enable users to produce and share digital content are collectively referred to as "social media." Digital material can be text, photographs, music, movies, and places, among other formats.[3] Social media has become a part of our everyday lives, with billions of people sharing massive amounts of data on sites like Facebook, Instagram, and Twitter on a regular basis. AI algorithms are used to analyze this data and behavior in order to give customers personalized information. Through the analysis of user-interacted articles, pages, and biographies, AI can identify patterns and recommend new content that people might find interesting. Content curation is a technique used to keep users engaged and entice them to stay on the platform longer.

Artificial intelligence has the potential to significantly alter how firms advertise on social media sites like Facebook, Instagram, Snapchat, Twitter, and LinkedIn. Campaigns, social media ads, and events may all be developed and targeted with it. It can automate regulation and powers the majority of content on social networks. At present, social media marketers may leverage this unadulterated technology to achieve incredible and long-lasting outcomes. The smartphone's voice assistants and real-time navigation are powered by AI. Online retailers, such as Netflix and Amazon, employ AI to recommend products and content. Email systems like Gmail even employ artificial intelligence to compose parts of your emails automatically.

Machine learning, a subfield of artificial intelligence that allows computers to reliably predict outcomes from massive volumes of data, which drives artificial intelligence's most impressive features. It is the most cutting-edge

---

[2] Matthew NO Sadiku and others, 'Artificial Intelligence in Social Media' (2021) 2 International Journal Of Scientific Advances <https://www.ijscia.com/?p=1906> accessed 10 February 2025.

[3] Muktesh Chander, 'Social Media: Analysis of New Challenges and Opportunities for Indian Law Enforcement Agencies' (2024) 2014 Indian Police Journal 123.

artificially intelligent tools available, whose forecast accuracy is getting better because AI can learn to get smarter on its own, often without human input, as it is incredibly powerful. Massive amounts of unprocessed data are used by AI technology nowadays to forecast increasingly relevant and precise outcomes, such as what product one should buy next, what advertising campaign to conduct, and what subjects to write about in a blog based on previous searches. Artificial intelligence can read and write through natural language processing and synthesis. It uses the sentiment analysis step to identify speech tonality. It recognises people, images, and videos using a variety of image recognition algorithms and computer vision techniques. AI is even able to forecast performance and suggest actions. And, by utilising these features, one can give the social media marketing superpowers and raise customer engagement.[4]

In order for social media platforms to function today, artificial intelligence is essential. Popular social networks such as Instagram, Facebook, LinkedIn, and others employ machine learning models to recommend users or accounts to follow, recommend jobs, identify photographs, monitor conversations, and do other similar functions. Artificial intelligence is used by several of the most well-known social networks that we utilise on a regular basis. Facebook employs more sophisticated forms of artificial intelligence and machine learning to display postings, among other things. They resemble those that a user has already interacted with. They can send pop-up advertisements, identify faces in tagged photographs, and so on. Facebook is the owner of the social networking site Instagram. To locate and remove phoney posts from user accounts, it employs AI. Snapchat tracks the traits of its users' faces in real time and adds effects that move with those features by using computer vision, a sort of artificial technology. LinkedIn leverages artificial intelligence for a variety of functions, including automated bidding, job recommendations, suggested connections, specialised content delivery in feeds, audience targeting assistance, and conversion tracking. The personalised content that Pinterest displays is a big part of why so many people adore it. Instead of typing in keywords, users can take photographs using Pinterest Lens and use them to search for relevant products. Because Pinterest provides hyper-personalized content, more than 80% of its active users make purchases through the platform.[5]

---

[4] Trupti Bansode and others, 'A Review On Impact Of AI On Social Media' (2024) 12.
[5] Preeti Singh and others, 'Implications & Impact of Artificial Intelligence in Digital Media: With Special Focus on Social Media Marketing' (2023) 399 E3S Web of Conferences 07006.

III. Hazards of Artificial Intelligence in Social Media

While AI has the potential to address some of the most difficult societal issues facing humanity, it is not a panacea. The possibility for privacy infractions in social media is one of the main hazards associated with AI. Social media sites have access to a great deal of personal data since AI algorithms use user data to personalise content and recommendations. Anything from location and search history to likes, shares, and comments might be included in this data. Although social media companies assert that they safeguard user privacy, there have been multiple cases of data breaches and improper use of user information in the past few years.[6]

The dissemination of false information on social media for political and social purposes is another issue. For nefarious political or financial purposes, a person could disseminate photos or films that were not authentic. Because so many politicians use forums to spread their opinions among the public, this dread has come to pass. The presence of AI-generated images and videos, AI voice changers, and fake news into political and social spheres has made online media and news even more depressing. Thanks to these technologies, users may easily generate realistic images, films, and audio snippets, or replace a current image in an existing picture or video with a new one and this technology is called "Deepfake".

Deepfake is a type of artificial intelligence (AI) technology that uses machine learning techniques, particularly generative adversarial networks (GANs), to produce synthetic media, such as images, videos, and sounds. The goal of deepfake technology is to create incredibly lifelike synthetic media that, with some content alteration, resembles real people. Deepfake technology is proliferating and ending up in the hands of unscrupulous people. Misuse of this technology can take the shape of dishonest business dealings, fictitious depictions of well-known individuals, and, in the worst situation, extortion. Over the last ten years, deepfake technology has advanced at an alarming rate and may be broadly classified into three categories:

a. Face switching - Face swapping is the practice of substituting another person's face for one's own in images or videos.

b. Lip Syncing - In audio or video content, lip syncing refers to the process of making someone appear to say something they did not say.

---

[6] 'The Biggest Data Breach Fines, Penalties, and Settlements so Far | CSO Online' <https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html> accessed 10 February 2025.

c. The puppet technique - This method describes the fake, phoney movements of a person.

Today, public at large is negatively impacted by Deepfake technology. Indian authorities recently dealt with their first case of impersonation using deepfake technology, which occurred in July 2023. An old man was conned out of his savings account by his bank when he received a deepfake video call from an AI-generated account that looked like it was from a colleague and asked for a big payment. Verification revealed that the video was a deepfake and that the aforementioned coworker was not aware of the video conference.[7] The issues with deepfake technology were once again brought to light when Bollywood actress Rashmika Mandanna's deepfake video began to circulate on social media.[8]

There are numerous ways that deepfake technology can be utilized to commit crimes. Although it can be used as a weapon to commit crimes against society as a whole, technology is not intrinsically dangerous. Crimes like identity theft and virtual forgeries can be perpetrated through the usage of deepfakes. These are grave offenses that have the potential to profoundly impact a person's life as well as society at large. By adopting another person's identity, fabricating personal narratives, or swaying public opinion, deepfakes can be used to disseminate misleading information and damage someone's credibility and reputation. Deepfake online defamation and hate speech can also be severe problems that hurt individuals and society at large. Deepfakes can seriously damage people's reputations, well-being, and online communities when they are used to disseminate hate speech or libellous content. Additionally, this technology can be used to create phoney images or videos of people saying or acting in ways that never happened, which could damage people's reputations or spread false information. Deepfakes may also be maliciously used for non-consensual pornography, political propaganda, or disinformation operations. Deepfakes can be harmful to society at large as well as the people whose images or likenesses are utilized without permission when they are used to spread false information or influence public opinion.

---

[7] 'Kerala Man Loses ₹40k to AI-Enabled Deep-Fake Fraud' (*Hindustan Times*, 18 July 2023) <https://www.hindustantimes.com/india-news/deepfake-scammers-trick-indian-man-into-transferring-money-police-investigating-multi-million-rupee-scam-101689622291654.html> accessed 10 February 2025.

[8] 'Rashmika Mandanna Deepfake Case: Delhi Police Writes to Meta to Give Info of Account That Shared Video' (*Hindustan Times*, 11 November 2023) <https://www.hindustantimes.com/entertainment/bollywood/rashmika-mandanna-deepfake-case-delhi-police-writes-to-meta-to-give-info-of-account-that-shared-video-101699689506970.html> accessed 10 February 2025.

IV. Legal Reforms for Deepfake AI Technology

Currently, India lacks in providing a specific law on Deepfakes and AI related crimes. But there is a plethora of different legal provisions that can provide for civil or criminal relief. Such as the defamatory laws in India, both criminal and civil law, can hold someone accountable for defamatory acts. Cyber defamation is the broadcasting of false information about another individual via the internet or computers. Cyber defamation occurs when someone posts a defamatory comment about another person on the internet or sends emails conveying the same to other people with the goal of discrediting the target of the statement.[9] In civil law, defamation is punishable by the tort law, which states that if the defamatory act is proven to have occurred, the person who was defamed will be entitled to damages. On the other hand, Section 499 of the Indian Penal Code, 1860, defines Defamation. According to this section, Defamation is a punishable offence and can result *"from publishing any material that could be construed as harming someone's reputation"*. Section 500 of the Indian Penal Code, 1860, stipulates the punishment for the same offence, which consists of *"a fine, a maximum two-year prison sentence, or both"*. These regulations are still in their infancy and cannot handle the variety of deepfakes that are currently in existence.

Cyber defamation was covered by previous cyber law as well, which was codified in Section 66A of the IT Act.[10] The clause specifically addressed any derogatory content delivered via a computer source with the intention of obstructing, offending, hurting, inciting hatred, intimidating criminals, or sowing discord. But this clause was removed from the IT Act as the Supreme Court invalidated it in the Shreya Singhal case.[11]

Section 66E of the IT Act presently applies to deepfake offenses that involve the acquisition, distribution, or publication of a person's image in the media, violating that person's privacy. This type of violations warrants a fine of ₹2 lakh or a jail sentence of three years. Similarly, Section 66D of the IT Act punishes those who maliciously use computers or communication devices to impersonate or deceive others. A violation of this provision carries a maximum sentence of three years in prison or a fine of ₹1 lakh.

Additionally, violating Sections 67, 67A, and 67B of the IT Act may lead to legal prosecution for transmitting or broadcasting pornographic or sexually explicit deepfakes. The IT Rules also prohibit hosting "any content that impersonates another person" and require social media companies to

---

[9] Aswathy Ph.D, 'A Critical Study on Cyber Defamation and Liability of ISPS' (2018) 119 International Journal of Pure and Applied Mathematics 1717.
[10] Information Technology Act, 2000.
[11] *Shreya Singhal* v. *Union of India* A.I.R. 2015 S.C. 1523.

take down "artificially morphed images" of people as soon as they are alerted. They risk losing the "safe harbour" protection, which exempts social media companies from legal responsibility for user-generated content on third-party platforms, if they fail to take down the aforementioned content.

Deepfake content occasionally includes modified audio and visual elements from movies or music videos that may be copyrighted. According to Section 14 of the Copyright Act of 1957, the owner of the cinematographed music video or film has the exclusive authority to provide a licence for the creation of another copy of the work, including any image or sound that is represented by a picture or photograph. The author's moral right was acknowledged in the Delhi High Court case of Amarnath Sehgal v. Union of India. In the event that his honour is violated or his moral rights over his creation are violated, the author is entitled to damages for any act of mutilation, distortion, or change. If the moral rights of his licenced work are violated, the copyright owner may be entitled to civil remedies such as an injunction, damages, or other remedies granted by the law. In addition, anyone found to have intentionally assisted in the infringement of a copyrighted work or any other rights granted to the copyright owner under the provisions of the Act faces up to three years in prison and a fine of up to two lakh rupees. However, these remedies might not be effective for the victim of a deepfake content because, generally speaking, it is believed that the producers of films own the copyright, not the actors, who run the risk of becoming targets. This also holds true for pictures and photographs, where the owner of the copyright is the photographer, not the subject of the picture. Therefore, neither the target of the deepfake content nor the real victim may benefit from the remedies offered by this act.

In the Justice K. S. Puttaswamy v. Union of India[12] case, the nine-judge bench acknowledged that an individual's right to privacy is protected under Part III of the Indian Constitution. The case centred on the individual's right to sue the State and non-state actors for infringements on their informational privacy, which acknowledges the individual's control over their personal and digital privacy. Therefore, utilising a person's private or intimate information such as pictures or videos to create non-consensual deepfake content about them is a violation of their fundamental right to privacy.

A historic piece of legislation was enacted in the shape of the Digital Personal Data Protection Act, 2023 (DPDPA) which seeks to protect people's privacy in the digital age. It aims to establish a comprehensive

[12] 2017 10 SCC 1.

framework for India's legislation pertaining to the protection of personal data. All organizations that handle the personal data of Indian persons are subject to the Act, which went into effect on September 1, 2023. The DPDPA attaches a Data Principle's obligations under Section 15 of the Act. Section 15(b) restricts the common problem of impersonation. This is important in light of AI-generative media, which is frequently used to deceive people by posing as someone else. Data Fiduciaries can track out the origin of a deepfake and hold the individual who uploaded it to the website accountable after receiving a complaint. This clause allows for action to be taken while providing the injured party with enough time to recover. However, this technique is only helpful when a person can be located using a unique identifier or a unique account on a data fiduciary platform. If this person impersonates someone else using a deepfake, they could be prosecuted for breaking Section 15. If it were difficult to identify the video's origin or link it to a specific individual, the clause would essentially be irrelevant.

V. Global Scenario

Deepfakes pose a serious risk to society at large, and as artificial intelligence has advanced, so too has its potential for evil. With the advancement of deepfake technology, it is now much easier to alter reality representations. Numerous social, economic, and psychological issues are brought on by deepfakes. India currently lacks a strong criminal legislation or civil liability framework that can directly address the problems associated with the production and dissemination of deepfake content. In a 2019 draft on intellectual property policy and artificial intelligence, the World Intellectual Property Organization (WIPO) addressed two specific concerns with deepfakes. This was accomplished in an indirect manner. The WIPO asserts that deepfakes have the potential to cause more significant issues, such as violations of human rights, privacy rights, and the protection of personal data, as opposed to copyright violations.[13]

a. Deepfake regulations in USA

The United States of America was in the forefront of the response to the advancement of artificial intelligence technologies. In 2018, the Malicious Deep Fake Prohibition Act was passed by the US Congress. This legislation is important since it is the first attempt to define the phrase “Deep-fake” legally. In 2019, the DEEP-FAKES Accountability Act was formally

[13] ‘Artificial Intelligence and Intellectual Property Policy’ <https://www.wipo.int/about-ip/en/artificial_intelligence/conversation.html> accessed 10 February 2025.

presented. The production and dissemination of deepfake films were outlawed in Texas in 2019, making it the first state in the union to do so. Following that, two laws were passed in California in 2019 that gave victims of deepfake, nonconsensual pornography the ability to sue for compensatory damages. The creation and distribution of non-consensual deepfake pornography are now crimes in Georgia and Virginia. Legislation connected to the pursuit of legal remedies against the unapproved spread of deepfake content was passed in New York in 2020.

b. Deepfake regulations in EU

The European Union (EU) is pushing for increased research efforts in the fields of deepfake identification and prevention, taking a proactive approach to the regulation of deepfakes. The European Union's Artificial Intelligence Act, 2024, has adopted a proactive approach in the fight against deepfakes. Furthermore, in order to combat deepfakes, the EU had previously suggested legislative provisions requiring the open labelling of artificially generated content, which have been appropriately acknowledged by the recently passed AIA. A thorough study titled "Tackling online disinformation: a European Approach" was issued by the European Commission in 2018. It featured a number of measures aimed at preventing information providers from unlawfully influencing public opinion.[14] In 2021, the Future of Science and Technology Panel conducted research and produced a report titled *"Tackling Deep-fakes in European policy."* The report detailed various aspects of the deep-fake lifecycle that policymakers could take into account to address and lessen the adverse effects of deep-fakes.

The General Data Protection Regulation (GDPR) of the EU has strict restrictions on deep-fakes. The definition of "personal data" in Article 4(19) of the law *is "any information that pertains to a specific or identifiable individual."* Given that a deepfake can be readily identified as a real person, it surely falls under the GDPR's purview if it does so. The EU has created the first comprehensive AI law in history, and it appears to be well-positioned to address the growing threat posed by deepfakes. This is in addition to the several regulations and initiatives now in place that attempt to incorporate deepfakes into the current legal framework. By taking these steps, the application of deepfake technology is limited with respect to artificial intelligence regulation, personal data protection, and misinformation

[14] ' Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236> accessed 10 February 2025.

governance. The most important AI regulatory framework for law enforcement in deepfakes is being developed by the European Commission, and its implementation is anticipated. Legislative steps have also been implemented by the EU to require social media companies to remove misinformation, including deepfakes, from their platforms.

VI. Conclusion & Recommendations

Technology is constantly evolving. There is a new development in the field of technology every day. AI is utilizing one such technology that has become popular. A wide range of technologies, such as computer vision, robots, expert systems, machine learning, natural language processing, and more, are referred to as "artificial intelligence." A lot of businesses are already aware that AI is the route to go in order to advance their operations. As AI advances and changes, social media networks will continue to be impacted by it. The possibilities are endless when it comes to AI in social media. Businesses have found social media and AI to be a particularly beneficial combination.

Deepfakes will continue to evolve and become more complex in the near future, which will raise concerns about how they might impact society. As AI algorithms advance, it becomes harder to distinguish between authentic and fraudulent content, which affects people, privacy, and trust. The likelihood of losing trust in digital content is rising as deepfakes become more realistic. When individuals begin to question whether any image or video is authentic, there may be a generalized sense of skepticism. This could have important ramifications in high-stakes domains like justice and law enforcement, where the integrity of the evidence is vital.

The spread of deepfake and shallow content highlights the need for sophisticated software and laws while also illustrating the evolution of deepfake technology. Examining synthetic media will require collaboration by lawmakers, IT developers, and the general public in order to achieve a balance between innovation and safeguarding against detrimental misuse. By doing this, we may all cooperate to safeguard the integrity of our digital environment and mitigate the negative consequences of deepfakes. When it comes to AI, the existing restrictions are insufficient. The legal system does not meet the needs of emerging technologies as it stands. Here are some suggestions to maintain the constant urge:

a. The state's existing laws against defamation, identity fraud, data theft, privacy, copyright, etc., should be reinforced in order to

combat the crimes linked to deepfakes. Strict sanctions and punishments for creating deepfake content may act as a check on the pace of technology development and the dangers it presents to society. It is necessary to pass laws that are directly related to AI and Deepfake technology.

b. When users encounter deepfake content on their network, social media apps, and service providers can develop and put techniques into practice to alert them. The terms and conditions of the service providers' privacy policies must set a limit beyond which they are unable to misuse the data and privacy of their customers.

c. Fighting deepfake content also requires education and awareness. The general public ought to be made aware of deepfake content and the potential risks associated with this AI-generated technology. Creating awareness among people not to share or promote any fake content online is another important aspect. The general public should be made aware of how to spot deepfake content that can be found on internet media platforms.

Well-known platforms like Facebook, Twitter, TikTok, Instagram, Snapchat, and others that let users upload and share content also have moral and societal obligations to forbid or restrict the publication of deepfake content. Since women make up the majority of those who fall victim to deepfake material, they are frequently the target of publications that publish non-consensual sexual content or any other type of deepfake content with the intention of harming or embarrassing them. It is imperative that these social media platforms maintain their integrity as a secure space for leisure for all users.[15] In order to facilitate users' ability to confirm the legitimacy of the media they come across, social media platforms ought to prioritise transparency in the content generation process. This could entail employing third-party validation tools for media integrity, watermarking, or other certification forms.[16]

[15] Srishty Dey, *Ethical and Legal Challenges of Deepfakes – An Indian Perspective,* III IJLSI 951-968 (2021).
[16] Neill Jacobson, 'Deepfakes and Their Impact on Society' (*CPI OpenFox*, 26 February 2024) <https://www.openfox.com/deepfakes-and-their-impact-on-society/> accessed 10 February 2025.