Quest Journals
Journal of Research in Humanities and Social Science
Volume 13 ~ Issue 7 (July 2025) pp: 191-197
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

Digital Arrest Using Artificial Intelligence Generative Deepfake Media Content in Post-Truth Society

Kawaljit Singh
Research scholar, Department of Journalism and Mass Communication, Maharshi Dayanand University, Rohtak. (Haryana)

Dr. Harish Kumar
Professor and Head, Department of Journalism and Mass Communication, Maharshi Dayanand University, Rohtak. (Haryana)

Abstract
In the present digital era, a new society is emerging, one that is often referred to as the post-truth society. In a post-truth society, facts are being eroded, and citizens are increasingly susceptible to fake information. Presently, in a post-truth society, deepfake media content can be produced with the help of artificial intelligence. Online schemers use Deepfake videos, photographs, and animated content to put victims under digital arrest. Cybercriminals create fake identities by cloning the voices of individuals and impersonating government officials to commit financial fraud.Due to an absence of awareness, the vast majority of victims fall into the situation of digital arrest. These frauds take advantage of victims' dread and uncertainty, leaving them both economically and emotionally ruined. Even intelligent people are also falling prey to these clever tactics: every day, headlines are filled with 'digital arrests' cases. The ethics and consequences of digital arrest are a source of ongoing controversy. Digital arrest has created concerns about privacy issues, surveillance overreach, and the possibility of misuse of power, raising red flags. Surveillance technologies, such as face recognition, have been criticised for having the potential to violate human rights and unfairly harm marginalised people.
This study provides critical advice on how to recognise and avoid falling victim to these cybercrimes, including techniques for validating information, securing personal information, and staying up to date on developing fraud.

Keywords: *Digital Arrest, Post-Truth Society, Artificial Intelligence, Deepfake, Cybercrimes*

R*eceived 15 July, 2025;* ***R****evised 28 July, 2025;* ***A****ccepted 31 July, 2025 © The author(s) 2025.*
Published *with open access at* ***www.questjournas.org***

I. Introduction

Digital extortion is a relatively recent phenomenon in which hackers use technology to instil fear and induce individuals to comply with their demands for money. Another more prevalent type of cyber scam is a digital arrest, in which fraudsters pretend to be governmental or regulatory officials and threaten victims via video or audio recordings of conversations. These criminals usually pose as law enforcement or other authorities, using fear and anxiety to coerce victims into transferring money or sharing personal information. The psychological impact of such attacks is profound and appropriate, leaving victims traumatised, isolated, and economically destroyed (Dr. Rajnish, 2024).Digital arrests have gained popularity as the digital economy has emerged with the advancement of technology. A digital arrest is the process of capturing someone virtually in cyberspace.The purpose of this digital attack is tocompromise someone's device for financial fraud and online harassment. It further led to personal identity theft, andsometimes by an enemy country for counterterrorism. In digital arrests, the victim is blocked from utilisinghis digital currency, tracking online conduct, and seizing personal electronic gadgets.

The Digital Arresthoax involves the government intercepting internet data and conversations to deter criminal activities such as hacking and cybercrime. Criminals are extorting money to conceal bogus judicial charges. This aids in detecting and preventing internet illicit actions. A digital arrest is a new type of cybercrime in which fraudsters call a potential victim and inform them that they have transported or are supposed to receive a package containing prohibited products, narcotics, fake passports, or any other banned item. Victims may be advised if they were involved in an offence or suffered an injury and have been imprisoned in jail. Scammers often demand payment as part of an offer of compromise. Victims may be subjected to "Digital Arrest" by fraudsters, requiring them to stay visible via Skype or video conferencing until their demands are met. Fraudsters sometimes pose in studios resembling police stations and government buildings, dressed in uniforms. Restricting people's internet access or conversations is similar to technological house arrest. (Asmita Mallick, 2024).OnOctober 27Prime Minister Narendra Modi raised the issue of "digital arrests" on his radio show “Mann Ki Baat” in this broadcast he warned people about digital arrest fraud. In his address, he asked Indian citizens to "Beware of digital arrest scams. He also concluded that "No government agency will ever contact you by phone or video call for such an investigation” toraise awareness about digital technology.

The digital arrest is a new type of internet fraud in which cybercriminals mislead individuals into believing they are under a digital or virtual arrest and induce them to continue communicating with the impostor via video conference technology. The scammers then persuasively convince their targeted individuals to keep a constant video correspondence, thus holding them captive to the crooks' bogus demands.

Objectives of the study

1. To do a phenomenological inquiry about “digital arrest” and its consequences in the present age.
2. To do a phenomenological inquiry about a post-truth society in which false information and deepfake content lure humans to indulge in digital arrest
3. To identify available legal remedies to prevent digital arrest.

II. Methodology

In the present study, the phenomenological inquiry method is adopted because a new concept of digital arrest has emerged. The concept of digital arrest is relatively new and has significant implications for the economy and the psychological aspects of a post-truth society. To move further with this study, a phenomenological inquiry is conducted based on relevant literature. How fraudulent minds use artificial intelligence technology to produce deepfake digital content and fake identities to put vulnerable individuals into digital arrest. Some available legal remedies are also taken into consideration, as there is no special law to counter digital arrest.

Phenomena of the Post-Truth society

The invasion of the media arena by false news and misinformation has pushed society into a post-truth state. It is claimed that as the impact of post-truth spreads over the media spectrum, people on its route may be carried along without raising the essential red signals that undermine the supposed strength and lifeblood of the emerging new media paradigm. Post-truthsociety lacks the ubiquitous potential to disorient. The post-truth society has reached a mental level where it is difficult to believe in facts. Truthful information began to decline, and false information became increasingly dominant. Individuals are not grouped in making essential media judgments whenever and wherever the need arises, regardless of the severity and frequency of bogus news they encounter. Thus, it is reasonable to conclude that post-truth cannot influence media users to the point where they abandon truth and objective facts in favour of 'alternative facts or falsehoods' in creating public opinion.A post-truth society is emerging and developing in response to the growing threat of misinformation. Now,apost-truth society isa media consumer living in a 'thinking cap' that allows them to figure out what is truthful and beneficial and what is bogus and unwanted (Olympus G. Ejue, 2024).

In common parlance, post-truth encompasses five interrelated concepts. Post-truth definitions emphasise the role of emotion in affecting personal ideas and public discussions, rather than objective facts. Post-truth refers to the relativisation of truth, implying that knowledge providers may manipulate political and scientific assertions. Politicians may contradict their previous statements without harming their reputations. As a result, a third feature of post-truth is a decrease in shame when exposed for factual errors or dishonesty. Fourth, this phenomenon appears to be associated with a propensity to polarise viewpoints. Manipulation of knowledge and polarisation of ideas often lead to 'conspiracy' notions (Malcolm, 2021).

AI-generated deepfake content as a tool for digital arrest

A digital arrest, similar to phishing attacks, involves deceiving a person into disclosing sensitive information, incurring financial loss, or having their information misused for illicit purposes. The approaches have advanced with the introduction of AI-generated video and audio content. Using live-conferencing programming, an individual can apply sophisticated deepfake videoconferencing technology to appear as a unique and frequently realistic human participating in the video conversation. In addition, utilising a clip of speech, such as from a judge or an upper-level law enforcement official, an audio AI algorithm can mimic an individual's tone of voice, which the fraudster can then implement (Oxford, 2024). Digital arrest has gained popularity in the modern digital age, driven by the rise of cybercrime and the need for a sophisticated judicial system to address criminals effectively. In recent years, internet usage has become an integral part of everyday life. Human financial transactions are also in digital form. This is the reason foran increase in digital crimes (Chauhan, 2024).

Although deepfake technology has existed since 2015, its application in fraudulent schemes has continued to increase in frequency and complexity as machine learning and other artificial intelligence methods have evolved.

Some of these innovative deepfake developments enable fraudulent scammers to produce audio clips or photographs, combining conversation using a deepfake AI, multimedia, and watching videos, and then hiding themselves as an actual individual in a virtual conference call via Zoom, Skype, or Teams. If the machine hosting the communication does not have anti-deepfake software, detecting the deepfake may be difficult.

Specific deepfake algorithms require only ten seconds to a minute of audio recordings of an individual conversing to mimic that individual's patterns of speech, emotions, and accent. Artificial intelligence software for speech will also handle realistic pauses, word inflexion,and tone of voice, producing a replica that can be considered virtually identical to the original speaker(Faqir, 2023).

2024 has witnessed an increase in fraudulent activities. Scams reached a never-before-seen level this year, driven by enhanced artificial intelligence (AI) capabilities, eroding public trust in organisations while inflicting significant financial losses on consumers.

According tothe Internet Crime Coordinating Centre, Indians lost an estimated Rs 11,000 crore to online fraud in the first half of 2024, with 6,000 complaints received daily on the National Cyber Crime Reporting Website. Every day, Indian victims claim losses of Rs 60 crore, as the level of sophistication and convincingness of AI-generated fraud advertising expands. The illegal use of artificial intelligence has additionally paved the way for new programs, including deepfakevoices used to fool loved ones and parents.

The strategy has been utilised to produce fake texts, impersonate voices in telephone conversations, create realistic graphics, and build deepfake videos.

AI-assisted speech duplication applications have been used to generate fraudulent replications of the accents of friends and family members, which criminals then used to steal money from victims (Sharma, 2024).

Economic Losses: Victims of "Digital Arrest" frauds face huge financial losses due to extortion, coercion, and fraudulent transactions perpetrated by cyber thieves. These financial losses affect not only individual victims but also the economy as a whole. Influencing consumer spending, investor confidence, and overall financial stability. Diverting resources to combat cybercrime and assist victims puts a burden on government budgets and financial institutions, compounding economic woes.

Psychological Trauma: Victimsof DigitalArrest frauds frequently report deep psychological trauma, worry, and stress as a result of hackers' pressure, intimidation, and manipulative methods. The social stigma associated with false charges of criminal activity can cause isolation, embarrassment, and reputational harm, aggravating the emotional toll on victims and families. Long-term psychological repercussions, including post-traumatic stress disorder (PTSD) and depression, may hamper victims' capacity to rehabilitate and return to normalcy in their lives (Vijay, 2025).

Types of digital arrests

1. **Cyberstalking:** Cyberstalking is a newdigital crime affecting our society. Cyberstalking isthe practice of following and pursuing someone online, breaching their privacy, and monitoring their every move. Harassment can disrupt a victim's life, making them feel unsafe and intimidated. In Cyberstalking crimes, scammers target women who are pursued or harassed by men. They also target childrenas adult predators or pedophiles. Cyberstalkers do not need to leave their homes to harass their targets and are not afraid of physical assault, as they feel they cannot be touched in cyberspace. Theystalk individuals using electronic communication channels on the Internet and e-mail (Deo, 2013).
2. **Hacking:**In the field of cybersecurity, computer hacking is the misuse of technology such as laptops, tablets, and smartphones to damage or hack systems, gain access to personal information, steal statistics, or disrupt data-related functions.
3. **Phishing:** Phishing is yet another kind of hacking. Phishing got its title from the term "phish," which means "fish." It is often done to lure the aquatic creature into becoming trapped. It is an unethical means of misleading the victim towards visiting hazardous websites. hackers try to get sensitive data such as credit card numbers, passwords, or account details from banks. Phishing can be accomplished through the transmission of falsified emails or messages that appear to be from trustworthy organisations, such as organisations or prominent websites.

4. **Cyberterrorism:**Digital terrorism is the use of internet means and strategies to commit acts of violence. It mainly refers to assaults motivated by political or ideological ideas and directed at computer systems, networks, or information storage infrastructure. The aims might range from disrupting services and obtaining personal information to causing bodily harm or inciting terror.
5. **Financial Fraud:**Financial fraud refers to illegal practices aimed at gaining financial resources or assets through deceit. Financial fraud may range from basic schemes to incredibly intricate and sophisticated operations, with dishonest individuals or organised criminal groups exploiting financial system vulnerabilities for personal gain.
6. **Child Exploitation and Pornography:**Digital pornography involving children describes the harassing or exploiting of a juvenile (under the age of 18) in a sexually graphic act or behaviour via pictures or videos posted online. Digital predators lurk on online social networking platforms, gaming sites, and chat rooms, attracting and luring children and adolescents into circumstances that result in sexual abuse or exploitation.
7. **Work-from-home scams:**Job-from-home scams have also increased in recent months, owing to the popularity of remote jobs and the large number of individuals seeking them. Scammers promise substantial rewards for basic activities, such as liking videos or completing simple tasks. They engage with victims using networks such as Telegram and WhatsApp, offering rich chances. Victims who fall into the trap need to pay a registration fee. Initially, little reimbursements are paid to victims to build trust. After trust, victims are asked to make investments and promise better profits. When victims attempt to withdraw their money, the fraudsters steal the money. To ensure security, thoroughly investigate work-from-home platforms, avoid making upfront payments, and verify the authenticity of firms through their official websites or testimonials.
8. **Illegal parcel scam:** Hackers take advantage of the current rise in e-commerce delivery to commit prohibited package fraud. As online purchasing becomes increasingly popular, fraudsters impersonate couriers or law enforcement authorities and call unsuspecting people. During the call, they frighten the victim by alleging that a box intended for him includes unlawful or restricted materials such as narcotics or weapons. They may conduct video calls while pretending to be police officers to boost their credibility.

Digital Arrests Case Studiesin India

1. **Bulli Bai App Scandal:**Mumbai police registered a case regarding digital arrests in 2021. Scammers were targeting Muslim women by publishing their photos for auction on Bulli Bai app. the attackers constructed fake identities with the advent of deepfake technology. This case warns of the perils of unregulated digital environments. This case raised serious privacy issues, and its creation ultimately led to its extinction, allowing us to learn about the complexity of this digital phenomenon and its far-reaching societal consequences. Cyber violence, as seen in this example, has targeted a small religious community of women who demonstrate assertiveness.
2. **Crypto Fraud Scandal:** Multiple scammers were arrested for defrauding investors via bitcoin fraud. Bogus cryptocurrency trading platforms were asking victims to invest in order to double their profits. Hackers promised investors high profits on Bitcoin investments. Hackers used blockchain analysis techniques to commit financial fraud. After receiving money, they ran away.
3. **Loan App Scams:**Some loan applications in Andhra Pradesh and Telangana engaged in extortion and harassment. Victims who took out loans using these apps were hounded by app operators, who accessed their contacts and sent nasty messages to their family members if they did not return on time. Law enforcement officials in India arrested numerous individuals suspected of involvement in these digital financial frauds after employing phone monitoring and digital payment forensics to track down the perpetrators.
4. **Sextortion Scams:**A sextortion gang was found in Gurgaon in 2021. Scammers exploited fictitious social media profiles and put victims into video conversations,and further recorded victims in uncomfortable positions. They would demand money after recording the video by threatening to broadcast it online.
5. **Investment Scams:** In 2024, scammers continued to target investments in Bitcoin, options, the stock market, and commodities. Scammers expanded their activities by utilising new investment opportunities, including the exploitation of brands and financial influencers, as well as dabba trading.In one example, fraudsters claimed to return three to four times the initial investment in just two hours on deposits as low as Rs 5,000. Investment scams often begin with the publication of fraudulent advertisements on social media sites like Facebook and Instagram, which entice individuals with offers of high returns on investment.

Legal Framework to PreventDigital Arrests in India

Indian citizen Gowrishankar, who lives in Bangalore, filed the PIL in the SC seeking a direction to the Department of Telecom and the Telecom Regulatory Authority of India to implement CNAP (Calling Name Presentation Service) to prevent cyber frauds.The Telecom Regulatory Authority of India launched the Calling Name Presentation Service as a feature that displays the caller's identity on the user's phone, which may help prevent spam and scam calls (PTI, 2025).

Currently, there is no direct law to address digital arrest. This term is not precisely used in the legal fraternity. India has made significant progress in combating digital crimes. There are some primary laws and regulations that governing presently to prevent digital arrests:

The Information Technology Act of 2000 serves as the foundation of India's cyber law system. The provisions of this act cover a wide variety of cybercrimes, including hacking, identity theft, and the online dissemination of objectionable material. This IT Act authorises law enforcement officers to investigate cybercrime-related cases and, after investigation, arrest and prosecute scammers for fraud. Under Section 66, officers can arrest individuals for unauthorised access and data theft related to computer offences.Section 67 addresses offences relating to indecent content. Section 69 authorises the government to intercept,analyse, or decode information for national security or cyber terrorism activity.Any scammer who illegally and knowingly exploits a person's digital signature, password, or any other unique identification characteristic will face punishment of up to three years and a fine of up to one lakh rupees.

Cybercrime punishments under BNS (Bharatiya Nyaya Sanhita)

The computer age and artificial intelligence have transformed human existence, impacting the daily lives of all of us today. However, despite the various benefits, the misuse of computers and artificial intelligence has resulted in cybercrime, or illicit activity carried out via electronic means. The Bharatiya Nyaya Sanhita, 2023 (BNS) imposes fines for various internet offenses. Cybercrime mainly began offline, but as technology advanced, it developed, posing challenges to data privacy, social interactions, and economic sovereignty.

Prevention of Cyber Crimes under BNS

Section 77 of BNS: This section covers the recording or broadcast of photographs of a woman's intimate parts or activities without her agreement, which constitutes voyeurism. This section helps to prosecute crimes related to sextortion.

Section 294 of BNS: Under this section, the production and dissemination of obscene content produced technologically are punishable with imprisonment and fines, with heavier penalties for repeat offences.

Section 303 of BNS: This section focuses on theft connected to mobile phones, data, and computer hardware/software. It provides a legal foundation for prosecuting persons who participate in cyber theft operations.

Section 318 of BNS: Address fraudulent activities such as password theft, the construction of phoney websites, and cyber fraud. Imposes varied sentences and penalties dependent on the degree of the offence.

Section 319 BNS: describes cheating by personation as deceiving people by claiming to be someone else, replacing one person with another, or portraying someone else or themselves. This offense applies even if the individual being impersonated is fictitious or deceased. It assures that people who perpetrate fraud via identity deception face legal consequences.

Section 336 of BNS: Addresses offences such as email spoofing and online forgeries that meant to harm someone's reputation. It can result in jail, fines, or both.

Section 351 of BNS: if the criminal persuasion can be committed by any individual who puts at risk another person with harm to their human being, public image, or property, or to their livelihood or repute.

Section 356 of BNS: Defamation is punishable, including the dissemination of defamatory material via email. Imposes jail and penalties.

Challenges Faced by Law Enforcement

1. Anonymity: Virtual Private Networks help scammers to hide their identity. Encrypted messaging apps and cryptocurrencies provide this anonymity. In this situation, law enforcement finds difficulties in identifying digital criminals.
2. Jurisdictional Issues: If the crime involves foreign actors, usually Cybercrimes often done by countries with cross-national borders, then it is difficult to prosecute perpetrators. It required international cooperation to resolve such cybercrime cases.
3. Lack of Resources: To deal with the rising number of cybercrimes, Indian law enforcement entities occasionally remain understaffed and digitally ill-equipped. Many cybercrime units lack the specialist equipment needed to perform electronic forensics, making digital arrests impossible to carry out successfully.
4. Evolving Technology: Cybercriminals continue to develop their methods in order to keep far ahead of law enforcement agencies. The development of new technologies, which include deepfakes, voice manipulation, and AI-powered attacks, poses novel challenges for entities responsible for executing digital arrests.
5. Legal Grey Areas: Digital crimes frequently bring up complex legal difficulties. Current regulations cannot encompass every aspect involved in creating technological advances, leaving gaps for criminals to exploit.

FuturePerspective of Digital Arrests in India

The number and severity of digital arrests are likely to increase as the Indian economy and social system become more electronically intertwined. We may witness the following developments:

1. Need New Cyber Laws: The Indian government has begun efforts on strengthening its cybersecurity laws to safeguard against emerging types of digital crimes, including digital arrest, deepfakes, and fraud using artificial intelligence.
2. Partnership with Foreign Organisations: In order to combat cross-border cybercrime, India will need further to develop its relationships with international law enforcement groups. Digital crimes occasionally involve hackers from different countries; thus, international collaboration is essential for effective enforcement.
3. Expanded Digital Forensics: Indian law enforcement continues to increase its expenditures in contemporary digital forensics innovations, cryptocurrency statistical analysis, and surveillance equipment powered by artificial intelligence to make cyber investigations more effective and precise.
4. Public Awareness: As more people in India become vulnerable to digital fraud, government agencies and cybersecurity agencies are expected to boost efforts to warn the public about the safety of the internet, scams, and how they can safeguard their digital identity.
5. Online monitoring: Sites such as Facebook, Instagram, and Twitter are becoming areas of concern for criminal activity ranging from hate speech to fraudulent transactions. Criminal justice utilises machine learning and AI systems to detect and respond to inappropriate behaviour on social media platforms in real-time.

Reasons why scammersachieve digital arrest

Lack of Knowledge: Many people are unaware of traditional law enforcement procedures, which makes them more likely to fall victim to scams.

Fear and fear: The threat of arrest induces fear, prompting victims to comply with requests. Victims demand immediate relief because of concern for reputational injury and the impact on family members (for example, children's futures).

Sense of Urgency: Scammers encourage victims to make quick decisions, preventing them from contacting others or investigating charges.

III. Conclusion

The rapid growth of technology presents considerable challenges for law enforcement authorities globally, particularly in combating cybercrime. Digital arrestencompasses the interaction of legal power, technical capabilities, and individual rights in the digital age. Digital arrest frauds pose a severe danger to Indians' financial and mental well-being. To address this issue, a comprehensive plan that includes improved law, technology, and education is essential, in addition to public awareness campaigns and government programs. To avoid digital incarceration, individuals should be informed about the ever-changing cyber danger and legislators should implement robust cybersecurity legislation. To eliminate cybercrime, people must adopt a proactive and vigilant approach to cybersecurity. Cyber hygiene techniques, including two-factor authentication and frequent password modifications, have become essential for decreasing the risk of unauthorised access to personal information. To avoid this growing danger, it is important that we promote media literacy all through all sections of society. Schools, educational institutions, technology firms, and media organisations ought to work together on establishing complete programs for literacy that provide people with the abilities people need to navigate the world of digital media.

Public awareness efforts and community workshops may assist to narrow the literacy gap. People ought to seek out different points of view and fact-check information to avoid the risks of deception, which are so common online.

References:

[1]. Asmita Mallick, P. G., 2024. Understanding Of Digital Arrest: Definition, Methods And Implications. *SSRN.*

[2]. Chauhan, J., 2024. Digital Arrest:An Emerging Cybercrime in India. *International Journal of Law Management & Humanities.*

[3]. Deo, D. S. S., 2013. CYBERSTALKING AND ONLINE HARASSMENT:A NEW CHALLENGE FOR LAW ENFORCEMENT. *Bharati Law Review,* pp. 87-93.

[4]. Dr. Rajnish, D. P., 2024. The Psychological Impact of Digital Arrest on Individuals: A New Threat to The society. *Library Progress International,* pp. 169-172.

[5]. Faqir, R. S. A., 2023. Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. *International Journal of Cyber Criminology.*

[6]. Malcolm, D., 2021. Post-Truth Society? An Eliasian Sociological Analysis of Knowledge in the 21st Century. *Sociology.*

[7]. Olympus G. Ejue, D. S. E., 2024. Post-Truth Society and the Social Media in The 21st Century. *Creative Artist: A Journal of Theatre and Media Studies.*

[8]. Oxford, D., 2024. *aljazeera.* [Online] Available at: https://www.aljazeera.com/news/2024/10/11/what-are-digital-arrests-the-newest-deepfake-tool-used-by-cybercriminals [Accessed 15 December 2024].

[9]. PTI, 2025. *SC issues notice to Centre on PIL over rising cybercrimes, spam calls,* s.l.: PTI.

[10]. Sharma, A., 2024. *India Today.* [Online] Available at: https://www.indiatoday.in/india/story/cyber-scam-in-india-digital-arrest-artificial-intelligence-2024-deep-fakes-2657439-2024-12-30 [Accessed 17 December 2024].

[11]. Vijay, B., 2025. The evolution of digital arrest cyber-crimes in India: Trends and patterns preventive measures. *International Journal of Sociology and Humanities.*