DIGITAL ARREST: A STUDY OF A RISING ORGANISED OFFENCE OCCURRING IN INDIAN CYBERSPACE

Mrinmoy Roy, LL.M., Department of Law, University of North Bengal.[1]

Arindam Dey, LL.M, Department of Law, University of North Bengal.[2]

ABSTRACT:

The digital revolution has transformed every aspect of contemporary society, from financial transactions and work to socialising and governance. India emerging as a digital economy in the globe, reliance on digital systems has surged. However, alongside these developments, cybercrime has developed into a corresponding threat that uses the same technological networks that empower our lives. Among the variety of cybercrimes, the emergence of Digital Arrest scams has surfaced as one of the major threats in recent years. Digital arrest is a scam which utilizes intimidation, coercion, deceit, and fear to extract money from victims. Fraudsters impersonate law enforcement officers and threaten victims with arrest, bank account freezing, and passport cancellation in order to get them to pay a sum of amount in order to abstain from being brought into legal action. The Indian Cyber Crime Coordination Centre (I4C) stated that in May 2024, an average of 7,000 cybercrime complaints were recorded daily, marking a significant surge of 113.7 per cent compared to the period between 2021 and 2023, and a 60.9 per cent increase from 2022 to 2023. To combat this growing crime, citizens need to be proactive and aware. Existing provisions like Section 204, 319, 336 of BNS, 2023 and Section 66C and 66D of IT Act, 2000 should be supported through more clear and classified legislations for these kinds of scams. Strict regulations should be issued by Department of Telecommunication for adequate identification of SIM Cards. Technological support should be there to detect, monitor and investigate the offences and mechanisms like AI Detection, spam alert, digital forensic tools should be adopted.

Keywords: Cyber Crime, Digital arrest, Scam, Intimidation, Coercion.

[1] Mrinmoy Roy, LL.M Student, Department of Law, University of North Bengal.
[2] Arindam Dey, LL.M Student, Department of Law, University of North Bengal.

INTRODUCTION:

The digital revolution has transformed every aspect of contemporary society, from financial transactions and work to socialising and governance. India emerging as a digital economy in the globe, reliance on digital systems has surged. However, alongside these developments, cybercrime has developed into a corresponding threat that uses the same technological networks that empower our lives. Among the variety of cybercrimes, the emergence of Digital Arrest scams has surfaced as one of the major threats in recent years. Although the term Digital Arrest sounds legal in nature, this crime is more accurately described as a type of cyber-enabled fraud.[3]

Recently, Prime Minister Narendra Modi addressed the nation in his 'Mann Ki Baat' and raised concern against the fraud of 'digital arrest'. He played an audio-video clip that showed a man in a police uniform, asking the victim to share his Aadhaar number to save his mobile number from being blocked. Unlike traditional arrests, digital arrest usually restricts a person from accessing his digital assets and freezing his physical movement by video calls.

Digital arrest is the name given to a cybercrime technique where defrauders send messages or make calls or video calls to manipulate the individual by impersonating law enforcement officials or investigating agencies and trapping them via deception involving threats of imminent digital restraint. Here cybercriminals claim that the individual or their family members have been found involved in criminal activities such as drug trafficking, money laundering or their Aadhaar card, SIM card or bank account has been linked to illegal activities and hence they are being arrested over video calls and sometimes pretend an online trial for such offence in court. They then force the victim to remain confined to the premises, instructing them to keep their laptop or mobile phone's camera on. All this is done to create panic in them, to demand money through online transfers to secure their release.

What particularly makes this scam insidious is the foreground of psychological manipulation; victims were monitored for hours using video surveillance, coerced into embarrassing themselves, and threatened with transferring large sums of money as 'security deposits' or 'penalties.' Fraudsters typically have elaborate processes to make the deception plausible; for example, they supply documents that appear fake, pretend to be speaking to the police, and

[3] N. Likhitha Prasad, *The Illusion of Authority: Understanding Digital arrest in India*, 1 C.L.R. 2, 5 (2025).

even fake a police station, often having staged a studio type of environment to make it convincing.

MEANING OF DIGITAL ARREST:

A person who is psychologically imprisoned, under pressure, or controlled by someone online is said to be under digital arrest, which leaves them open to abuse or damage. Digital arrest is a scam which utilizes intimidation, coercion, deceit, and fear to extract money from victims. Fraudsters impersonate law enforcement officers and threaten victims with arrest, bank account freezing, and passport cancellation in order to get them to pay a sum of amount in order to abstain from being brought into legal action.[4]

In other words, Digital arrest is a cybercrime involving scammers posing as law enforcement officials (for instance, as officials from Reserve Bank of India, Central Bureau of Investigation or Directorate of Enforcement, etc.) and falsely accusing the victim of committing a crime. These scammers often attempt to isolate the victim and subsequently leverage the threat of fictitious consequences, such as arrest or imprisonment, to extort significant sums of money or part with personal information to prevent supposed legal action.

The scam typically begins with a phone call - seemingly innocent at first, offering everything from a harmless parcel delivery claim to a demand for KYC verification. As the conversation progresses, the scammer uses increasingly aggressive tactics to in still panic, often claiming that the victim is involved in serious crimes like money laundering, cybercrime, or drug trafficking. With fake documents, doctored videos, and even spoofed phone numbers, the scammers create an air of legitimacy, pushing the victim to comply with their demands.[5]

THE RISE OF DIGITAL ARREST:

In the last 10 years, internet use has increased dramatically in India, a country with a population of over one billion. According to the government report in Sansad Unstarred Question No. 2351, answered on 15th March 2023, the total number of internet users in India,

[4] https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf , (last visited Aug 09, 2025).
[5] Ibid.

spanning both rural and urban areas, has reached 850.95 million.[6] Millions of Indians are now connected in ways they never imagined because of the proliferation of cell phones, social media, and internet commerce. Millions of Indians are now connected in ways they never imagined because of the proliferation of cell phones, social media, and internet commerce. While this digital transformation has many positive aspects, it has also created opportunities for new forms of criminal activity, such as digital arrests. The potential severity of cybercrimes increases with the extent to which we utilise technology for communication, including social media and banking and debit card transactions. Possibilities for cybercrime are growing as technology permeates every aspect of life, from social media to finance. A Government report submitted to a Lok Sabha questioning (Unstarred Question No. 2504) cites data from the Ministry of Home Affairs that indicates an upsurge in cybercrime incidents reported into categories involving communication instruments between 2020 and 2022, headed from 50,035 in 2020 to 65,893 in 2022. The urgent necessity for effective cybersecurity for protecting citizens from such online attacks is demonstrated by this growing trend. According to data provided in answer to Lok Sabha Unstarred Question No. 2082, serious financial loss results from incidents like credit card, ATM/debit card, and internet banking frauds. The Reserve Bank of India (RBI) lost ₹177.05 crores in the 2023–2024 fiscal year, which is a substantial amount in contrast to the ₹44.22 crores it lost in the 2019–20 fiscal year.[7] This significant increase underscores the heightened vulnerabilities individuals face in digital financial transactions and the importance of safeguarding the digital environment to prevent financial harm. To safeguard people's rights and maintain the security of the digital environment, it is essential to understand what digital arrests entail in this context.

Cybercriminals may readily prey on the unwary in a country where millions of individuals are still unaware about the effects of the Internet. The Indian Cyber Crime Coordination Centre (I4C) stated that in May 2024, an average of 7,000 cybercrime complaints were recorded daily, marking a significant surge of 113.7 per cent compared to the period between 2021 and 2023, and a 60.9 per cent increase from 2022 to 2023.[8] A single click, a password, or even an arbitrary

[6] Government of India, Ministry of Communications, Department of Telecommunications. (2023, March 15). *Internet connectivity in rural areas* (Lok Sabha, Unstarred Question No. 2351). Retrieved from https://sansad.in/ls/questions/questionsand-answers

[7] Government of India, Ministry of Finance, Department of Financial Services. (2024, August 5). Unstarred Question No: 2082, Answered on Monday, August 5, 2024/14 Shravana, 1946 (Saka). Lok Sabha. https://sansad.in/ls/questions/questions-andanswers

[8] Business Standard. (2024, May 27). Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024. www.business-standard.com. https://www.business-standard.com/india-news/here-is-how-much-indians-lost-tocyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html

social media post may plunge someone into a digital hole. The repercussions for those who have not yet received any cybersecurity education can be severe, affecting their professional, social, and intimate lives. When we consider the devastating consequences suffered by the victims - those who are frequently left helpless by their anguish and suffering in the middle of their online selves - the need to lessen these digital traps becomes even more pressing.

'Arrest' is no longer a tangible occurrence due to the velocity of the digital transition; instead, it has established itself in the realm of digital virtual walls. Understanding the socio-legal aspects of this phenomenon - that is, how cybercriminals take advantage of technological flaws and human frailties to gain psychological and digital control over their target.

RECENT SCENARIOS OF DIGITAL ARREST:

- In a recent case of 'digital arrest', cyber criminals pretending to be police officials allegedly kept two lady's captive on a video chat for almost nine hours and made them strip naked for an online medical examination reported on 23 July 2025.[9]

- A cybercriminal was caught in Ahmedabad, Gujarat, for defrauding an elderly person out of Rs 49.88 lakh by pretending to verify his account, after placing him under digital arrest for 'being involved in a Rs 300cr scam'.[10]

- Malti Verma, a teacher at a government school in Agra, tragically passed away in a misfortune linked to a well-known cybercrime due to digital arrest. Because it took advantage of her desire to parent and her sentiments of affection for her kid, among other things, the scam serves as an incident of the psychological injury that may arise from cybercrime. Digital abuse in this case study can be just as deadly as physical violence.

  On September 30, 2024, an individual impersonating a police officer often and unsettlingly phoned Malti Verma. Under the guise of "Captain Vijay Kumar," the scammer took advantage of Verma's weakness to fool her into thinking her daughter

[9] https://timesofindia.indiatimes.com/business/cybersecurity/digital-arrest-scam-two-women-held-on-hostage-for-near ly-nine-hours-by-fraudsters-posing-as-police/articleshow/122862160.cms, & https://timesofindia.indiatimes.com/business/cybersecurity/digital-arrest-scam-two-women-held-on-hostage-for-near ly-nine-hours-by-fraudsters-posing-as-police/articleshow/122862160.cms , accessed on 20 August 2025.
[10] https://timesofindia.indiatimes.com/city/ranchi/cyber-fraud-held-from-abad-for-scamming-elderly-of-50l/articlesho w/122819893.cms , accessed on 20 August 2025.

was involved in a sexual scandal and demanded a sum of Rs. 1 lakh to release her. The situation worsened further when the cyber-criminals threatened that Verma could still not talk to her daughter nor reveal the matter to anyone else.[11]

- A 48-year-old contract staffer with Bescom, who fell prey to the digital arrest fraud and lost nearly Rs 13 lakh to cybercriminals, was found hanging from a tree in his village in Ramanagar district reported on 16 July 2025.

  K Kumara, a resident of HSR Layout in Bengaluru, has explained in the death note the harassment he faced from the fraudsters, who posed as CBI officials, and repeatedly threatened him with arrest if he failed to pay up. He was found dead near an agricultural land at Kelagere village in Channapatna.[12]

- An elderly couple lost Rs 50 lakh in a 13-day digital arrested in Madhya Pradesh's Khandwa. The accused cyber fraudsters trapped the couple by posing as DSP.

  The criminals forced the couple to break their fixed deposits and later took an extra ₹70,000 in the name of bail.[13]

- In Rohini, Delhi, a horrifying digital scam destroyed the life savings of a 72-year-old retired engineer, totalling over Rs 10 crore. A horror scenario that demonstrates how even the most vigilant person might fall victim to technology is "Digital Arrest" fraud. It's a highly complex fraud. This scam started when the victim received a phone call informing them that an allegedly Taiwanese parcel had been discovered to contain illegal drugs at the Mumbai airport. The scammers intensified the issue right away by posing as police and threatening to arrest the old guy if he disregarded their orders.

  Scammers impersonating police officers forced the victim to join a Skype video conversation and then drove them to be on call for hours without dropping the call. They told him that if he moved or turned off the camera, he would be arrested right

[11] The420.In. (2024, October 3). Death In Digital Arrest: Mother Dies of Heart Attack After Cyber Criminals, Impersonating Police, Demand Rs 1 Lakh for Daughter's Fake Release from a Sex Racket. The420.in. https://the420.in/death-in-digital-arrest-mother-dies-of-heart-attack-after-cyber-criminals-impersonating-police/

[12] https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-man-hangs-himself-after-losing-rs-13l-to-digital-arrest -fraud/articleshow/122586844.cms , accessed on 20 August 2025.

[13] https://www.freepressjournal.in/indore/madhya-pradeshs-elderly-couple-loses-50-lakh-in-13-day-digital-arrest-cyber-crooks-posed-as-dsp-forced-them-to-break-fd , accessed on 22 August 2025.

away, and worse, his family would be held accountable. The engineer obeyed, frightened and alone. As the video chat went on, a second scammer who was impersonating a Mumbai Police officer won his trust and persuaded him to move his money to other "safe" accounts in order to stay out of trouble with the law.[14]

- An 86-year-old woman from south Mumbai lost more than ₹20 crore of her savings over two months to a 'digital arrest' fraud, police said on Thursday (March 20, 2025).[15]

- Three persons including two senior citizens kept under digital arrest by cyber frauds who posing as officials of Mumbai police threatened them with drug smuggling and money laundering before robbing a total of Rs.1.8 crore from them.[16]

- Scammers deceive an industrialist out of ₹7 crores by faking a Supreme Court hearing and impersonating the Chief Justice of India (CJI).[17]

LEGAL PROVISIONS AGAINST DIGITAL ARREST:

The astonish rise of Digital Arrest Scam has poses a significant challenge to Government machineries and enforcement agencies in India. During the time from 2022 to 2024 Digital Arrest scams and other cybercrime scam have increased by 3 times marking the amount of defrauded increased by 21 times. By 2024, the reported cases rose to 1,23,672 and total monetary amount reached to Rs. 1935 Crores. In first 2 months of 2025, total 17,718 new cases have been reported, calculating to Rs 210.21 crore of monetary losses.[18] There are direct laws against this evil threat however, there are laws which indirectly cross paths against these activities:

[14] https://www.indiatoday.in/cities/delhi/story/delhi-man-retired-engineer-duped-crore-digital-arrest-scam-2633687-2024-11-15 , accessed on November 15,2024.
[15] https://www.thehindu.com/news/cities/mumbai/elderly-woman-loses-20-crore-to-digital-arrest-fraud-3-held/article69353437.ece
[16] https://www.countryandpolitics.in/2025/08/22/three-including-two-senior-citizens-kept-under-digital-arrest-by-cyber-frauds-posing-as-mumbai-officials-threatening-to-foist-false-drugs-money-laundering-case-robbed-rs-1-8-crore-in-seperate-cases/ , accessed on 02 October 2025.
[17] https://www.livelaw.in/top-stories/scammers-fake-supreme-court-hearing-impersonate-cji-dupe-industrialistof- 7-crore-271253, accessed on 24 August 2025.
[18] FE News Desk, *Massive spike in digital arrest scams, cybercrimes almost tripled: Govt,* FINANCIAL EXPRESS (Mar. 12, 2025, 08:06 PM), https://www.financialexpress.com/india-news/massive-spike-in-digital-arrest-scamscybercrimes-almost-tripled-govt/3775959/ [*FE News Desk*].

Offence under Bharatiya Nyaya Sanhita, 2023:

Section 111- Organised Crime[19]: According to sub-section (1) an organised crime is constituted when any continuing unlawful activity which includes robbery, extortion, kidnapping, economic offence, cyber-crimes, trafficking of persons etc. is committed by a group of persons jointly or by a single person, through use of violence, threat, coercion intimidation or other lawful means, as a member or behalf of an organised crime syndicate to obtain indirect or direct material benefit.

Explanations (i) explained "organised crime syndicate" as a group of 2 or more persons jointly or singly involved in a continuing unlawful activity. Explanation (ii) states "continuing unlawful activity" as an activity which is a cognizable offence punishable for imprisonment of at least of 3 years and more than 1 charge sheet have filed and cognizance has been taken by competent court for such offence within last 10 years. Explanation (iii) explained "economic offence" as any scheme including forgery, criminal breach of trust, criminal breach of trust, counterfeiting of Government stamps or any other scheme to defraud several persons or financial institutions or banks or other organisations.

Punishment: According to sub-section 2(b), if any organised crime is committed for which death has not been then the offender shall be liable with both imprisonment which shall not be less than 5 years but extendable to life imprisonment and fine which shall not be less than Rs. 5 lakhs.

As a member: Under sub-section 4, if any person is merely a member of such syndicate, he shall be liable with both imprisonment which shall not be less than 5 years but extendable to life imprisonment and fine which shall not be less than Rs. 5 lakhs.

Possession of Property: According to sub-section 6, if any person possesses the property obtained from such organised crime shall be liable with both imprisonment which shall not be less than 3 years but extendable to life imprisonment and fine which shall not be less than Rs. 2 lakhs.

Possession of behalf of syndicate: Under sub-section 7, if any person possesses any immovable or movable property on behalf of organised crime syndicate and which has no

[19] Bharatiya Nyaya Sanhita, 2023, § 111, No. 45, Acts of Parliament, 2023 (India).

satisfactory account shall be liable with both imprisonment which shall not be less than 3 years but extendable to imprisonment of 10 years and fine which shall not be less than Rs. 1 lakh.

It has been found that in a case of digital arrest the accused were 8 members' gang. They ran 24 shell companies to launder their money. The defraud money were around Rs. 159 crores from victims across India. The accused obtained hundreds of SIM cards and used them to create fake WhatsApp accounts. The foreign links also have been found. This is the case where digital arrest was conducted by an organised crime syndicate. It was a continuous unlawful activity as multiple FIRs were filed within the span of 10 years regarding same offence occurred across India. The sheer amount of money makes it an economic offence as through this scheme the accused defrauded several persons, financial institutions and banks, making it an organised crime.[20]

Section 204- Personating Public Servant[21]: If any person knowingly pretends to hold any office of public servant or falsely impersonate any other person who is holding such office and commit or attempt to commit any act under the colour of such office shall be liable with imprisonment which shall not be less than 6 months or may extend to 3 years and fine. The offenders present themselves as public servant to threat the victims that they are under official custody. Thus, this provision will apply.

Section 205- Fraudulently wearing garb or carrying token of public servant[22]: If any person knowingly and fraudulently wears any garb or carries token used by a certain class of public servant with the intention or knowledge that he may be believed as a person belongs to that class of public servant shall be liable with imprisonment up to 3 months or fine up to Rs. 5 thousand or both. To make themselves genuine the offenders were garb of police officers, judicial officers, custom officers. Hence, this section would be applicable.

Section 319- Cheating by Personation[23]: Any person who cheats by pretending to be some other individual or by substituting one person with another person or by representing himself or any other person as some other person shall be committing cheating by personation.

---

[20] HT News Desk*, 'Digital arrest' scams: ED reveals eight-member gang's modus operandi, I4C issues fresh advisory,* HINDUSTAN TIMES (Nov 03, 2024, 3:26 PM), https://www.hindustantimes.com/india-news/digital-arrest-scams-ed-reveals-eight-member-gangs-modus-operandi-issues-fresh-advisory-101730624381161.html.
[21] Bharatiya Nyaya Sanhita, 2023, § 204, No. 45, Acts of Parliament, 2023 (India).
[22] Bharatiya Nyaya Sanhita, 2023, § 205, No. 45, Acts of Parliament, 2023 (India).
[23] Bharatiya Nyaya Sanhita, 2023, § 319, No. 45, Acts of Parliament, 2023 (India).

Section 336- Forgery[24]: According to sub-section 1, a person said to commit forgery, if he makes any false document or electronic record or part of these to cause injury or damage to any person or public or to support any title or claim or to cause any part of property or to enter into implied and expressed contact or with the intent to commit fraud. Sub-section 2 talks about punishment of forgery i.e. imprisonment up to 2 years or fine. Sub-section 3 increases the punishment up to 7 years along with fine if the person commits forgery of documents or electronic records to be used for cheating. Sub-section 4 states that if a person commits forgery with the intention or knowledge of harming the reputation of any person then he shall be punished with imprisonment up to 3 years and fine. Sometimes the offenders show fake seals, electronic records, orders and notices to establish their credibility as an officer, making it forgery under this act.

Section 351- Criminal Intimidation[25]: Sub-section 1, defined Criminal Intimidation as any act where a person threaten another person with any injury to him or any interested person or to their reputation or property and cause him to do any act which he is not legally bound to do or to omit any act which he is legally bound to do for avoiding the execution of such threat. Sus-section 2 deals with punishment which is imprisonment up to 2 years or fine or both. Sub-section 4 states if any person caused criminal intimidation through anonymous communication or takes any precaution to conceal his name or source from which such threat comes shall have additional punishment of imprisonment up to 2 years for such offence. Being arrest is an attack over social reputation of the victim and to avoid this stigma the victims often agreed to do such things they are not bound to do by law to avoid the actual execution of arrest. Due to this digital arrest also comes under criminal intimidation.

Offence under Information Technology Act, 2000:

Section 66C- Punishment for Identity Theft[26]: According to this provision if any person dishonestly or fraudulently uses any unique feature for identification such as signature, password or other means of any other person then he shall be liable with both imprisonment up to 3 years and fine up to Rs. 1 Lakh. In Digital Arrest the offender often uses the name, signature or other fake documents to make him identifiable as an official personal thus, will be

[24] Bharatiya Nyaya Sanhita, 2023, § 336, No. 45, Acts of Parliament, 2023 (India).
[25] Bharatiya Nyaya Sanhita, 2023, § 351, No. 45, Acts of Parliament, 2023 (India).
[26] Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India).

guilty under this provision.

Section 66D- Punishment for Cheating by Personation by using Computer Resource[27]: According to this provision if a person cheats his personation as somebody else by the use of computer resource or any other communication device shall be liable with imprisonment up to 3 years and fine up to Rs. 1 lakh. The offender uses mobile phones to deceive the victim through voice or video call and present himself as police or other official personal. Hence, he shall be liable under this Section.

Combination of BNS, 2023 and IT Act, 2000:

Section 319 of BNS punishes the offender for cheat by personation and Section 204 punishes for personation of public servant while Section 66D of IT Act, 2000 deals with cheating through personation by using computer resources. In the cases of digital arrests, the offender uses cheating by personation of public servant and they use computer resources like mobile phones, laptop, tablet etc. Hence, violating the provisions of both of the acts and combination of both Acts can be an effective mechanism against these offences. On the other hand, Section 205 of BNS deals with fraudulently wearing garb or carrying token of public servant and Section 336 of BNS talks about forgery which can be applicable more effectively if it combined with Section 66C of IT Act, 2000 which deals with Identity theft of electronic records. It may happen that that the offender who wears garb of any public servant also provides false electronic records to make the victim believe that he is a person who is officially holding the possessing which falls under the purview of both of the Acts. In these ways the both BNS, 2023 and IT Act, 2000 can complement each other to fill the gaps contain in each of the Acts individually.

Relevant Provisions under Bharatiya Nagarik Suraksha Sanhita, 2023:

Section 35(3)- Person who may be arrested without warrant[28]: This provision states that the police officer shall issue a notice to the accused person to appear before him or any placed given in such notice who is under reasonable suspicion in committing cognizable offence.

Section 63- Form of Summons[29]: It stated that every summon shall be in writing, signed and seal of Court and duplicated as per the rules. However, it can be in a form of encrypted or other

[27] Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).
[28] Bharatiya Nagarik Suraksha Sanhita, 2023, § 35, No. 46, Acts of Parliament, 2023 (India).
[29] Bharatiya Nagarik Suraksha Sanhita, 2023, § 63, No. 46, Acts of Parliament, 2023 (India).

form of electronic communication bearing an image of seal of Court.

Section 64(2) Summon how served[30]: It states that summons shall be as far as practicable be served personally to the concerned person and provide him a duplicate copy of it. But it also stated that summons can be served through electronic communication provided by State Government if it bears the image of court seal.

Section 179(1)- Police officer's power to require attendance of witnesses[31]: It states that the if it appears to investigating officer that a person is acquainted with the fact and circumstances of the case then, he can make an order in writing required such person to be appeared before him. The section also gives relaxation to a person under 15 years, mentally and physically disable persons and woman.

Section 195- Power to Summon[32]: It provided same power as given under Section 179 to the police officer investigating any suicide case under Section 194. It also provides similar exceptions as given in Section 179.

***Satender Kumar Antil v. Central Bureau of Investigation[33]*:** Statutory formalities must be observed be police official while serving a notice under Section 35(3) of BNSS. The court refused to serve notice through electronic mediums like email, WhatsApp etc and should be given in person. The case was not about digital arrest yet it focused upon the traditional service along with procedural safeguards anticipating the probable misuse of this provision.

CASE LAWS OVER DIGITAL ARREST:

Re: Victims of Digital Arrest Related to Forged Documents Case:[34]

A Suo-moto case initiated by Hon'ble Supreme Court of India over a complaint filed by a senior citizen who was defrauded through digital arrest scam. His entire life saving was lost in this scam. The Court directed the intermediaries to provide full assistance to CBI regarding the

[30] Bharatiya Nagarik Suraksha Sanhita, 2023, § 64, No. 46, Acts of Parliament, 2023 (India).
[31] Bharatiya Nagarik Suraksha Sanhita, 2023, § 179, No. 46, Acts of Parliament, 2023 (India).
[32] Bharatiya Nagarik Suraksha Sanhita, 2023, § 195, No. 46, Acts of Parliament, 2023 (India).
[33] Satender Kumar Antil v. Central Bureau of Investigation, (2022) 10 SCC 51.
[34] Re: Victims of Digital Arrest Related to Forged Documents vs Mr. Avishkar Singhvi and Ors., Suo Moto Writ Petition Criminal No(s). 3/2025.

investigation as per Intermediary Guideline Rule of 2021. The Court also directed the Ministry of Home Affairs to constitute a high-level committee to counter this threat.

Mandate of MHA Committee: Hon'ble Supreme Court directed the Ministry of Home Affairs to constitute a high-level committee to under the chairmanship of Special Secretary. The prime task of this committee will be to examine the issues faced by enforcement authorities in investigating cases related to digital arrest scam which includes coordination issues, jurisdictional problems, difficulties in finding digital footprints, delay in information flow etc.[35]

Jatin Anup Ladwal and Ors v. State of West Bengal:[36]

In this case the petitioner was 74 years retired professor who lost his money including fixed deposits, PPF, gold loan, mutual fund investments being trapped in digital arrest scam. He received WhatsApp call from an unknown number and called himself as sub-inspector of Mumbai Police. It was found by the Kalyani Sessions Court that the case involved multiple accused who are habituated in these kinds of cybercrimes and also have foreign link. The 9 accused were found guilty for digital arrest and other online scams. The accused were jointly held liable in furtherance of common intention of all members, criminal conspiracy, fraud, cheat by personation, forgery and criminal breach of trust.

Re: In the matter of tackling the issue of 'Digital Arrest Scams' Case, 2025:

In this case Rajasthan High Court defined the "Digital Arrest" in a more concrete manner. It explained digital arrest as deceptive and sophisticated form of cyber fraud where the offenders present themselves to the victim as law enforcement agencies to extort money from them. The offender used tactics like threat, manipulation, intimidation, coercion to extract huge sum of money from the victim.

Thes scams are executed in a systematic manner through emails, phone calls or video conference. To break it down in following works:

[35] Debby Jain, *Digital Arrests | Banks, Telecom Cos Be Held Liable If Victim's Loss Attributable To Their Negligence: MHA Committee,* LIVELAW (Jan. 15, 2026, 10:06 AM), https://www.livelaw.in/top-stories/supreme-court-digital-arrests-victim-compensation-inter-departmental-committee-mha-liability-of-banks-telecoms-victim-loss-negligence-fraud-519132.

[36] Jatin Anup Ladwal and Ors v. State of West Bengal, Cyber Crime P.S. Case No. 61 of 2024.

1. **Initiating Contact:** The offenders accuse the victim that he is under investigation of a serious offences like money laundering, drug trafficking to pose immediate fear in the mind of the victim.

2. **Instilling Fear:** The offenders threaten the victim to comply with their demands failing to do so shall pose serious enforcement action against them.

3. **Creating a Facade of Legitimacy:** To present their credibility the offenders wear fake uniform, use fake identification card and forge documents. They even create government office environment to deceive the victim.

4. **Isolation Tactics:** The Victims are often instructed to keep their camera and microphone "on" through out the interaction creating a difficult position to seek any assistance. This method also isolates the victim to increase the fear and urgency in mind.

The Court urges the government to use mass communication to spread people aware about these scams and guide them to communicate to enforcement machineries if they encounter any of such scams.

Related Case Laws:

Justice K.S. Puttaswamy (Retd.) v. Union of India[37]*:* The Hon'ble Supreme Court of India in this case affirm right to privacy as a part of fundamental right under Article 21 of Constitution. It also empathises upon dignity, liberty and autonomy over physical and informational dimension. When the victims are compelled and isolated by the offenders it would pose direct threat to privacy and individual liberty of the victim. It also restricts the movement of the victim causing violation to his freedom of movement under Article 19 of Constitution.

DK Basu v. State of West Bengal[38]***:*** The Supreme Court provided different procedural safeguards to the arrested person against the enforcement malpractices. While digital arrest complete destroys these safeguards by using coercion against the victim making him vulnerable.

[37] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[38] DK Basu v. State of West Bengal, AIR 1997 SC 610.

People's Union for Civil Liberties (PUCL) v. Union of India[39]: The Court struck down the provision of telephone tapping posing safeguard against arbitrary actions of government servants. It also upheld right to privacy and dignity of an accused. The digital arrest scam attacks the very foundation of procedural mandate of the victim.

LEGAL CHALLENGES OF DIGITAL ARREST:

The Term "Digital Arrest" is not included in the Indian legal system, it has become one of the most prominent issues in the country's cybercrime landscape. This fraudulent scheme has caused significant financial losses by having cybercriminals pose as law enforcement officials and falsely assert that they have the authority to make arrests via digital technologies. There have been almost 92,000 reported incidents of digital arrest scams as of January 2024, resulting in an astounding Rs 2,140 crore in lost revenue.[40] Even though there isn't a special law on "digital arrest," these schemes are part of the mix of current criminal offences, such as mental harassment, online blackmail, and cyber extortion.

Since there isn't a single rule on digital arrest, Indian law enforcement has had to deal with these offences by combining several different legal systems. The Information Technology Act of 2000 (IT Act) and provisions of the Bhartiya Nyaya Sanhita (BNS) are the main legal frameworks for prosecuting offences related to digital arrest, particularly those involving fraud, extortion, and blackmail. For example, cyber offences are covered under **Section 66** of the IT Act. **Sections 66C and 66D** deal especially with identity theft and online impersonation, which are prevalent in these frauds). Also, if the criminals use obscene threats or obscene content to intimidate their victims, **Section 67** of the IT Act, which addresses providing or sending obscene content electronically, could also be pertinent.

Another significant challenges in digital arrest is the delay in **accessing and transmitting information.** Digital data relevant to a crime is often stored with internet service providers (ISPs), social media platforms, cloud service providers, and telecom companies. These entities may be located in different jurisdictions, sometimes outside the country where the crime is investigated. Before accessing such data, investigating agencies must comply with legal

[39] People's Union for Civil Liberties (PUCL) v. Union of India, AIR 1997 SC 568.
[40] *Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024*. www.business-standard.com. https://www.business-standard.com/india-news/here-is-how-much-indians-lost-tocyber- frauds-between-jan-and-apr-of-2024-124052700151_1.html , accessed on May 27,2024.

procedures, including search warrants, court orders etc. This procedural delay often results in the loss, destruction of crucial electronic evidence, making arrest difficult or even impossible.

Another challenge in 'digital arrest' is the difficulty in **identifying and tracking digital footprints**. Unlike traditional crimes, cyber-crimes do not always leave visible or physical traces. Criminals often operate behind screens, usernames, and virtual identities, which are deliberately designed to hide their real identity. Cyber offenders frequently use Virtual Private Networks (VPNs), proxy servers, Tor networks, and spoofed IP addresses to conceal their location. As a result the digital trail often leads investigators to false or misleading locations complicating the process of arrest.

One of the main challenges of Digital Arrest is Digital crimes frequently involve **cross-border elements**. The offender, victim, and digital infrastructure may all be located in different countries. This creates complex jurisdictional issues because Countries has many differences in Cyber Laws, Investigation process and Foreign policies. This often creates delay in digital arrest.

Another serious challenge in digital arrest is the lack of **timely and effective communication** between law enforcement officers and banks or other financial institutions. In most cybercrimes such as online fraud, phishing, identity theft and money laundering financial transactions form the core evidence. However, delays and procedural process in obtaining financial data significantly effects the arrest process. Banks and financial institutions are bound by banking laws, customer confidentiality obligations, and data protection regulations. As a result, they cannot immediately share account details, transaction histories, or beneficiary information without formal legal authorization. Investigating agencies are often required to obtain court orders, written requisitions, or approval from senior authorities, which consumes valuable time. By this delay, criminals may withdraw, transfer, or launder the money, making arrest and recovery difficult.

SUGGESTIONS:

The government, State police and telecom regulatory authorities should work in cooperation with each other to support prompt action and coordination to detect, monitor and investigate these kinds of unlawful activities. The government also take initiative to spread public awareness through the use of social media, seminars, advertisements, radios and other mass

communications to prevent these unlawful activities. The social media platforms should be obliged to provide all kind of technical assistance to the public servants during investigation such offence take place in their platform through messages, voice call, images or video conferences.

The Department of Telecommunication should impose stricter regulations and verification mechanisms for SIM cards. Technologies like call masking detections, real time blocking of suspected number and prompt communication to the police service should be adopted. Banking and other financial platforms should adopt technological supports like AI content detection, spam alert, cooling period before the completion of transaction. There should be prompt communication and reporting methodologies between banks and enforcement agencies for real time detection and monitoring of such scams.

There is need of clear classification of such scams for which Standard Operating Procedures (SOPs) should be adopted for quick response whenever these crimes are detected. More Technological assistance should be given to the local enforcement agencies to detect, counter and supervise over such anti-social activities taking place in the cyber space for which better trained personnel, forensic tools and inter-state coordination are required to be embraced. Strengthening and streamlining of reporting process and victim supporting mechanisms should be upheld. National Cybercrime Helpline Numbers 1930 and Cybercrime Portal should be simplified through more user-friendly approaches. Along with immediate account-freeze mechanisms, legal aid and psychological support should be provided to the victims to ensure timely reporting and stress management.

CONCLUSION:

Digital Arrest scam is rising in India for which prompt actions are needed to be taken by the government. During the time from 2022 to 2024 Digital Arrest scams and other cybercrime scam have increased by 3 times marking the amount of defrauded increased by 21 times. By 2024, the reported cases rose to 1,23,672 and total monetary amount reached to Rs. 1935 Crores. In first 2 months of 2025, total 17,718 new cases have been reported, calculating to Rs 210.21 crore of monetary losses.[41] The rise of digital arrest is a notable threat to the cyber security of any nation. The fraudsters take advantage of people's unawareness and weakness

[41] *FE News Desk, Supra* note 1 at 1.

either in personation or by coercive measures. They use tricks over victims that they are in danger of suffering harsh legal repercussions and thereby take large amounts of money from them. They often use fear as a powerful tool to manipulate individuals and to exploit their vulnerabilities to commit this crime. To combat this growing crime citizens need to be proactive and aware. Existing provisions like Section 204, 319, 336 of BNS, 2023 and Section 66C and 66D of IT Act, 2000 should be supported through more clear and classified legislations for these kinds of scams. Strict regulations should be issued by Department of Telecommunication for adequate identification of SIM Cards. Technological support should be there to detect, monitor and investigate the offences and mechanisms like AI Detection, spam alert, digital forensic tools should be adopted. There must be proper communications between financial institutions, police services, cyber cells for prompt reporting and identification of offence. Citizens must know about this constantly changing cyber threat with knowledge and educated practices and legislature must enact strong cyber security laws. National wide programmes should be held for better public awareness.

REFERENCES:

i. N. Likhitha Prasad, The Illusion of Authority: Understanding Digital arrest in India, 1 C.L.R. 2, 5 (2025).

ii. https://www.niti.gov.in/sites/default/files/202504/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf , (last visited Aug 09, 2025).

iii. Government of India, Ministry of Communications, Department of Telecommunications. (2023, March 15). Internet connectivity in rural areas (Lok Sabha, Unstarred Question No. 2351). Retrieved from https://sansad.in/ls/questions/questionsand-answers

iv. Government of India, Ministry of Finance, Department of Financial Services. (2024, August 5). Unstarred Question No: 2082, Answered on Monday, August 5, 2024/14 Shravana, 1946 (Saka). Lok Sabha. https://sansad.in/ls/questions/questions-andanswers

v. Business Standard. (2024, May 27). Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024. www.business-standard.com. https://www.business-standard.com/india-news/here-is-how-much-indians-lost-tocyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html

vi. https://timesofindia.indiatimes.com/business/cybersecurity/digital-arrest-scam-two-women-held-on-hostage-for-nearly-nine-hours-by-fraudsters-posing-aspolice/articleshow/122862160.cms , &

vii. The420.In. (2024, October 3). Death In Digital Arrest: Mother Dies of Heart Attack After Cyber Criminals, Impersonating Police, Demand Rs 1 Lakh for Daughter's Fake Release from a Sex Racket. The420.in. https://the420.in/death-in-digital-arrest-mother-dies-of-heart-attack-after-cyber-criminals-impersonating-police/

viii. https://www.freepressjournal.in/indore/madhya-pradeshs-elderly-couple-loses-50-lakh-in-13-day-digital-arrest-cyber-crooks-posed-as-dsp-forced-them-to-break-fd

ix. https://www.thehindu.com/news/cities/mumbai/elderly-woman-loses-20-crore-to-

digital-arrest-fraud-3-held/article69353437.ece

x. https://www.livelaw.in/top-stories/scammers-fake-supreme-court-hearing-impersonate-cji-dupe-industrialistof- 7-crore-271253

xi. FE News Desk, Massive spike in digital arrest scams, cybercrimes almost tripled: Govt, FINANCIAL EXPRESS (Mar. 12, 2025, 08:06 PM), https://www.financialexpress.com/india-news/massive-spike-in-digital-arrest-scamscybercrimes-almost-tripled-govt/3775959 [FE News Desk].

xii. Bharatiya Nyaya Sanhita, 2023.

xiii. HT News Desk, 'Digital arrest' scams: ED reveals eight-member gang's modus operandi, I4C issues fresh advisory, HINDUSTAN TIMES (Nov 03, 2024, 3:26 PM), https://www.hindustantimes.com/india-news/digital-arrest-scams-ed-reveals-eight-member-gangs-modus-operandi-issues-fresh-advisory-101730624381161.html.

xiv. Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India).

xv. Satender Kumar Antil v. Central Bureau of Investigation, (2022) 10 SCC 51.

xvi. Re: Victims of Digital Arrest Related to Forged Documents vs Mr. Avishkar Singhvi and Ors., Suo Moto Writ Petition Criminal No(s). 3/2025.

xvii. Debby Jain, Digital Arrests | Banks, Telecom Cos Be Held Liable If Victim's Loss Attributable To Their Negligence: MHA Committee, LIVELAW (Jan. 15, 2026, 10:06 AM), https://www.livelaw.in/top-stories/supreme-court-digital-arrests-victim-compensation-inter-departmental-committee-mha-liability-of-banks-telecoms-victim-loss-negligence-fraud-519132.

xviii. Jatin Anup Ladwal and Ors v. State of West Bengal, Cyber Crime P.S. Case No. 61 of 2024.

xix. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

xx. DK Basu v. State of West Bengal, AIR 1997 SC 610.

xxi. People's Union for Civil Liberties (PUCL) v. Union of India, AIR 1997 SC 568.

xxii. Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024. www.business-standard.com. https://www.business-standard.com/india-news/here-is-how-much-indians-lost-tocyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html