HIGH COURT OF JUDICATURE FOR RAJASTHAN

BENCH AT JAIPUR

In Re : In the matter of tackling the issue of 'Digital Arrest Scams', Cyber Crimes and saving the innocent people from loosing their money and lives.

JUSTICE ANOOP KUMAR DHAND

ORDER

22/01/2025
Reportable

By the Court:

1. Day in and day out it has been observed by this court in several electronic, print and social media reports that over the last few years, Cyber Crimes and the offences like 'digital arrest' have increased worldwide and in our country thousands of innocent people have been trapped in it and they have lost huge amount of their hard earned money and also lost their lives. Increase of 'digital arrest' cases have been highlighted the alarming rise of such scams targeting the individuals from every walk of life.

2. 'Digital arrest' is a new and innovative tactic employed by scammers/cybercriminals to defraud gullible victims and extort money. The modus operandi in this cybercrime method is that fraudsters pose as law enforcement officials such as Police, Enforcement Directorate, CBI, etc. and manipulate them into believing that they have committed some serious crime.

3. The scammers deceive the victim into believing that he or she has been put under 'digital arrest' and will be prosecuted if he/she does not pay the scammers an amount of money as demanded by them. As per cyber experts, the fraudsters in this

tactic are using fear and sense of urgency against the victims and ensure that they part with their money before they realize that it is a scam. Cyber criminals/scammers often use Artificial Intelligence (AI) to scare victims by mimicking voice of their loved ones and family members in order to extort money from them.

4. They often force the naive victims to self-arrest or self-quarantine themselves, by tricking them into believing that they have been put under 'digital arrest' and cannot leave their house unless they pay to amount as demanded.

5. In the age of rapid digital evolution, digital arrest scams have emerged as one of the most insidious forms of cybercrime. Scammers frequently exploit vulnerability gaps within the digital spaces, using themes of authority, urgency and fear to trick victims into revealing personal information or transferring money. Different countries have implemented variety of methods to combat this rising threat with varying level of success.

6. The term ‘digital arrest’ refers to a sophisticated and deceptive form of cyber fraud wherein criminals pose themselves as law enforcement officers or government officials to extort money from innocent persons. These scams employ manipulative psychological tactics, often leading victims to believe they have been implicated in serious criminal activities. Under the duress of threats and intimidation, victims are frequently coerced into paying huge amount of money to evade severe consequences such as arrest or incarceration.

It is important to note that ‘digital arrest’ has no legal standing in India. Digital arrest represents a highly sophisticated scam that can snare even well-educated individuals.

7. Digital arrest is the act of instilling fear and panic in individual, before extorting money from them under false pretenses, ultimately making such individuals a victim of cybercrime.

8. Digital arrest scams typically unfold in a systematic manner, with fraudsters reaching out to the victims through various channels such as phone calls, emails or video conferencing. Here is a breakdown of how these scams generally work:

1. Initiating Contact: Scammers accuse victims of their direct involvement in serious criminal offences, like drug trafficking or money laundering, creating an immediate fear in the minds of the victims.

2. Instilling Fear: By threatening victims with arrest in case they fail to comply with their demands, scammers effectively manipulate their emotions, posing a sense of urgency and fear.

3. Creating a Facade of Legitimacy: To lend credibility to their claims, fraudsters go to extreme ends. They use phony uniforms, counterfeit identification cards, and forged documents. In some cases, they operate from simulated government office environments, further persuading victims of their authenticity.

4. Isolation Tactics: Victims are often instructed to keep their cameras and microphones in “on” mode throughout the scam interaction, making it

difficult for the victims to seek assistance or discuss the situation with anyone. This tactic lies at the heart of the scammers' strategy, as it isolates victims, enhancing fear and compliance.

9. When the world is increasingly reliant on digital interactions, understanding the mechanisms behind digital arrest scams is essential for safeguarding oneself against such threats. Awareness and education are crucial in recognizing the signs of such attacks, ensuring that individuals remain vigilant and informed, thereby reducing the likelihood of falling victim to these scams.

10. **International Responses to Digital Arrest Scams**

1. Legislation and Regulatory Measures

Many countries have bolstered their legal frameworks to address digital arrest scams. For instance, **Australia** has enacted laws that focus on enhancing penalties for identity theft and cybercrime. The Cybercrime Act was amended to increase the penalties for telecommunication fraud scams, which helps authorities to act against scammers more effectively. Notably, in 2021, Australian authorities had arrested a group of individuals who were orchestrating a large-scale scam operation that defrauded victims of over AUD 3 Millions, showcasing the requirement of effective legal intervention.

2. Public Awareness Campaigns

Creating awareness among the public is a cornerstone of combatting digital scams. The United States has launched extensive campaigns through the Federal Trade Commission (FTC) and the Internet Crime Complaint Centre (IC3). These campaigns educate citizens on recognizing the telltale signs of scams, the importance of safeguarding personal information, and reporting such scams. Recently, FTC in assistance with local law enforcement agencies hosted workshops and webinars, which resulted in increased reportings from citizens regarding scams, helping track down and dismantling several scams.

3. Collaborative Efforts Between Agencies

Collaboration between governmental agencies and private companies is essential for combating digital scams effectively.

4. Technological Solutions

Technological advancement can also play a crucial role in combating digital arrest scams. Singapore has implemented AI-driven solutions powered by the Cyber Security Agency (CSA) to detect and block scam calls before they reach potential victims. This system utilizes machine learning algorithms to identify patterns based on historical scam data. In 2023, Singapore's Ministry of Home Affairs reported a reduction in scam cases by 25% following the implementation of these technological

measures.

5. Hotlines and Reporting Platforms

Establishing dedicated hotlines and online reporting platforms enables victims to report incidents swiftly, allowing authorities to track scam trends and identify hotspots. Canada has deployed the Canadian Anti-Fraud Centre, which provides a toll-free hotline for reporting scams. For instance, in 2022, a spike in digital arrest scams was noted, prompting the centre to launch an emergency communication strategy, resulting in the arrest of several individuals in a coordinated effort to target scammers operating across provinces.

6. International Cooperation

Digital scams often cross borders, making international cooperation vital. Organizations like INTERPOL and EUROPOL have created task forces that facilitate sharing of information and joint operations. In 2023, a multinational operation led by INTERPOL against a syndicate involved in digital arrest scams across Asia and Europe resulted in the arrest of 80 individuals and seizure of assets worth in millions.

11. The National Crime Record Bureau (NCRB) report complies and publishes the statistical data on crimes in its publication "Crimes in India". The last report published in the year 2022

reveals that around 65,893 cases related to cyber crime were registered through out the country and around 1,833 cases were registered in Rajasthan and these offences have added the new offence of 'digital arrest' and the same is increasing day by day.

12. In order to curb this new crime 'Digital Arrest' several advisories have been issued at the Government level and even some steps have also been taken.

13. The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs (MHA), coordinates activities related to combating cybercrime in the country. MHA is closely working with other Ministries and their agencies like RBI and other organizations to counter these frauds. I4C is also providing inputs and technical support to Police Authorities of States/UTs for identifying and investigating the cases. The I4C has issued an alert to the police in all the States and Union Territories amid the surge in the cases of digital arrest."

14. Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by on boarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh in 2023.

I4C has also blocked more than 1,000 Skype IDs involved in such activities, in collaboration with the Microsoft. It is also facilitating blocking of SIM cards, Mobile devices and Mule

accounts used by such fraudsters/scammers. I4C has also issued various alerts through infographics and videos on its social media platform 'Cyberdost'.

15. The MHA's cyber wing has also set up a helpline number to report such cases and seek more information about the new menace of cyber-crime. Victims have been asked to call 1930 and immediately report such frauds to the I4C wing.

16. The National Cyber Forensic Laboratory (Investigation) has been established, as a part of the I4C, at New Delhi to provide initial cyber forensic assistance to Investigating Officers (IOs) of the State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) has provided its services to State Law Enforcement Agencies in around 9,000 cyber forensics like mobile forensics, memory forensics, Call Data Record (CDR) Analysis, etc. to help them in investigation of cases pertaining to cyber crimes. **National Cyber Forensic Laboratory (Evidence)** has been set up at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber crime, preserving the evidence and its analysis in line with the provisions of the Information and Technology Act and Evidence Act; and reduced turnaround time.

17. Additionally, Massive Open Online Courses (MOOC) platform, namely **'CyTrain' portal** has been developed under I4C, for capacity building of Police Officers/Judicial Officers through online course on critical aspects of cyber-crime investigation, forensics, prosecution etc. along with certification. More than 76,000 Police Officers from States/UTs are registered and more than 53,000 Certificates have been issued through the portal.

18. The MHA has also provided financial assistance to the tune of Rs. 131.60 crores under the **'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme**, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of Law Enforcement Agencies personnel, Public Prosecutors and Judicial Officers. Cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs and as on June 2024, more than 24,600 Law Enforcement Agencies personnel, Judicial Officers and Public Prosecutors have been provided training on cyber crime awareness, investigation, forensics, etc.

19. Additionally, the Department of Telecommunications (DoT) has issued an advisory to citizens in wake of surging cases of cyber fraud, urging citizens not to attend fake phone calls. It has advised people to stay vigilant and report such fraud communications at '**Chakshu - Report Suspected Fraud Communications' facility of Sanchar Saathi portal** (www.sancharsaathi.gov.in/sfc). The DoT also advises citizens to report at cyber-crime helpline number 1930 or www.cybercrime.gov.in in case of already a victim of cyber-crime or financial fraud. Citizen can report such calls at Chakshu facility available on the Sanchar Saathi platform by providing details about suspected fraud calls, SMS and WhatsApp messages including screenshot, medium of receipt, category of intended fraud, date and time of receiving such communication. The Chakshu facility is a significant step taken towards safeguarding citizens from cyber fraud. By providing a streamlined process for

reporting suspicious activities, it helps in the early detection and prevention of potential frauds, thereby protecting users from financial and personal losses.

20. Further, in response to the mushrooming of aforementioned threat, the DoT, in collaboration with Telecom Service Providers (TSPs), has introduced an advanced system designed to identify and block incoming international spoofed calls before they can reach Indian telecom subscribers. This system is being deployed in two phases: first, at the TSP level, to prevent calls spoofed with phone numbers of their own subscribers; and second, at a central level, to stop calls spoofed with the numbers of subscribers from other TSPs.

As of now, all the TSPs have successfully implemented the system. About one third of total spoofed calls at 4.5 million spoofed calls are being stopped from entering the Indian telecom network. The next phase, involving a centralized system that will eliminate the remaining spoofed calls across all TSPs, is expected to be commissioned shortly.

21. The State of Rajasthan has also taken several steps to curb cybercrime, including **'Operation Anti-Virus'** and setting up of **Centre for Cyber Security**. Operation Anti-Virus is a collaboration between the Rajasthan Police, the Government of India, and the DoT. Herein, Rajasthan Police conducted this operation last year in 2024, targeting a group involved in fraudulent activities and the same resulted in the arrest of multiple suspects. The Police have blocked various suspicious SIMs and mobile phones and arrested cyber criminals involved in extortion and fake investment schemes.

22. Further, the Government of Rajasthan has set up a Centre for Cyber Security Centre at the Sardar Patel University of Police at Jodhpur, with the aim to develop Information Security roadmap for the State of Rajasthan and help the departments of Rajasthan Government including large/medium/small scale units to ensure implementation and awareness of Information Security, and develop a centre of excellence in the area of cyber security and further providing training to government and non-government agencies by carrying out onsite as well as offsite workshops/seminars in the field of Information Security.

23. Digital arrest scams pose a significant threat in our interconnected world, necessitating a multi-faceted approach to combat them effectively. Different countries have adopted legislation, public awareness campaigns, technological innovations and collaborative initiatives to mitigate the risks associated with these scams. While challenges remain, ongoing efforts and commitment at local, national and international levels signify a promising trajectory toward reducing the prevalence and impact of digital arrest scams. The shared experiences and strategies from various nations serve as crucial learning points in this ongoing battle against cybercrime. Ultimately, empowering individuals with the knowledge and tools to resist such scams will be paramount in this fight.

24. Though several steps have been taken at the various levels of the Government but in order to curb out the current and dangerous situation more serious steps are required to be taken by all the stakeholders.

25. Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (for short 'Rules of 2021') have been enacted by the Government to control the activities of social media platforms, over the top platform and digital news portals. These Rules track out the source of damaging information. It has been found that datas are sold by some of the social media companies and the same are misused by the accused involved in committing such cyber crimes with the innocent public at large. Our country's growing technical progress and increased penetration are reflected in the rise of cyber crime in the nation.

26. It is right time and high time to spread a public campaign through print, electronic, social media, television and FM Radio every hour and every day to make the public at large aware that there is no provision for law enforcement to conduct 'arrest is via video calls or online monitoring'. If the public receive such calls, it is a clear scam. In fact, the recently enacted new criminal law does not provide for any legal provisions of conducting digital arrest. The Bhartiya Nagrik Suraksha Sanhita, 2023 (BNSS) s for the summons to be served electronically under Section 63. The section defines the form of summons. It states that every summons served electronically shall be encrypted and bear the image and seal of the Court and digital signature. The people must be made aware of the fact that as per Sections 35 & 36 of BNSS, due process at the time of arrest has to be followed. The police officer carrying on the arrest has to be accurate visible and clear identification and prepare a memo of arrest at the time of arrest, which is required to be attested at least by one witness and signed by the person being arrested.

27. Some serious steps are required to be taken at the level of Reserve Bank of India (RBI) to not to transfer the money of such trap transactions or stop payment of such fraudulent transaction in every case where complaint is made/lodged by the sufferer/victim.

28. The RBI and the Government is required to develop a mechanism of stoppage of payment to the fraudulent person wherever complaint is received on the portal or website or mobile number to the Complaint Redressal Committee, so that the money of innocent people can be saved.

29. Taking a serious note of this alarming situation and increase of this new cyber crime, a *suo moto* cognizance is taken by this Court and the same be registered as:-

Suo Motu : In the matter of tackling the issue of 'Digital Arrest Scams', Cyber Crimes and saving the innocent people from loosing their money and lives.

Vs.

1) Union of India, through Secretary, Ministry of Home Affairs, New Delhi.

2.) National Cyber Forensic Laboratory (Investigation & Evidence), through its Director, New Delhi.

3) Reserve Bank of India, through its Governor, New Delhi.

4) National Payment Corporation of India, through its Director, New Delhi.

5) Chief Secretary, Government of Rajasthan, Secretariat, Jaipur.

6) Director General of Police, Police Headquarters, Jaipur.

7) Additional Director General of Police (Cyber Crime), Police Headquarters, Jaipur.

30. Issue notice to the respondents, making the rule returnable by three weeks.

31. The Chief Secretary, Government of Rajasthan, Jaipur; and Secretary, Ministry of Home Affairs, New Delhi are directed to submit a report before this Court regarding the steps taken by the State and Central Government to curb out from the situation arising out of these offences of digital arrest and cyber crime.

32. This Court requests Mr. R.D. Rastogi, Additional Solicitor General of India, Mr. Rajendra Prasad, Advocate General and Mr. Anurag Kalavatiya, Advocate, to assist this Court on the issue involved in this petition. Office is directed to provide a copy of this order to them.

33. Office is directed to place this matter before the Hon'ble Chief Justice for its listing before the appropriate Bench.

(ANOOP KUMAR DHAND),J

Karan/