Page 1632 - 1646 **DOI:** *https://doij.org/10.10000/IJLMH.118669*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 6

2024

Digital Arrest: An Emerging Cybercrime in India

JYOTI CHAUHAN[1]

ABSTRACT

"Arrest signifies physical detainment, none can be arrested digitally as there is no such concept in India"

The complex and contentious issue of digital arrest has gained attention in modern digital world due to proliferation of cybercrime and need of an advanced legal mechanism to deal with the offenders. In recent years, internet usage and digital services have abruptly arisen, resulted rise in digital crimes. The central theme of this paper is to highlight the tricks by which cyber-crooks extort money and the legal regime regarding the offence in India. This work is basically done by using case study method wherein certain incidents of digital arrest and its background is studied.

To explore the subject in depth and to know about awareness of people regarding this issue, it follows a doctrinal research approach, a survey has also been conducted in a close ended questionnaire form by using qualitative method. The work starts with defining the term digital arrest, how it works and the legality of digital arrest in India. It also deals with the legal framework for digital arrest and technology used to combat it. This work throws light over certain treaties which assures fundamental right of privacy at online platforms. Coming to end the challenges faced by law enforcement agencies and some suggestions for protection of internet users are discussed. In the end author sum up with concluding remarks.

Keywords*: Block-chain, digital forensic, digital arrest, cyber-crooks, digital surveillance, data interception, cyber-crime syndicate.*

I. INTRODUCTION

India witnessed that internet usage and digital services have abruptly arisen, resulting in a hike in digital crimes. 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

[1] Author is a Research Scholar at Jiwaji University, India.

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.

(A) Research Methodology:

The combination of doctrinal and non-doctrinal methodologies can provide a more comprehensive understanding of the law and hence this research follows both methodologies together. In this work doctrinal method of research is applied and using this method, a descriptive and detailed analysis of legal rules found in primary sources like cases, statutes and regulations have been dealt with. It helped in spreading basic awareness of legal issues among the people. In this research descriptive information is collected by using a case study method wherein certain incidents of digital arrest and their backgrounds are studied. To explore the subject in depth and to know about the awareness of people regarding this issue, it follows a survey method and is conducted in a close-ended questionnaire form. A survey method in a close-ended questionnaire is a type of question that limits the respondents to predetermined answers, in this method respondents are asked to choose from a predetermined set of responses, typically as 'yes or no', 'true or false or a set of multiple-choice questions. They are also known as qualitative questions. It aims to develop a theory from the collection of experiences and follows an inductive approach. An inductive approach or inductive reasoning is a method of concluding by specific observations and then drawing a general conclusion from them.

II. Crimes leading to digital arrest

There are certain acts if committed either by the victim or defrauder, invite the offence of digital arrest against victims, they are:

- **Hacking:** It is unauthorized access to computer systems or networks of people and by hacking accounts offenders use it in violation of any law or legal obligation and thereafter intimidate victims by pretending to be law officials and defrauding money from them imposing penalties on them by indulging them in fake trials.

- **Cyber-stalking and Online Harassment:** These cybercriminals have a keen eye over people and have access to their social accounts sometimes even to intimidate individuals they use digital platforms to harass, stalk, or threaten them or even commit so by the account of victim itself.
- **Phishing:** Phishing is fraudulently acquiring sensitive information like passwords, financial details etc. of individuals showing defrauders as trustworthy entities and thereby using them in certain ways to defraud money via threat to arrest digitally.
- **Pornography:** The distribution or creation of porn content whether it involves minors or not, is an offence. People often unknowingly pick up such calls on which some porn content is shown to them and once such call is dropped, these offenders immediately call such person alleging them to involve in pornography.
- **Financial Fraud:** Crimes like credit card theft, identity theft and other offences of like nature are also committed against victims to intimidate them. Here false allegation of illegal payment from their account is made against them and hence tried to trap them in this offence.
- **Fake News and Hate Speech:** The dissemination of false information or incendiary content through the account of the victim makes them fall in the gist of this offence. These offenders generally track the online activity of their prey or their close relatives weeks before making such fraudulent calls.

III. LEGALITY OF DIGITAL ARREST IN INDIA

The Indian Cyber Crime Coordination Centre issued a public advisory in connection with the increasing cases of 'digital arrest' crimes in India. In the advisory, the panel said law enforcement agencies such as the CBI, police, customs, ED, or judges do not conduct arrests through video calls and cautioned the public against falling victim to these schemes.[2] There is no legal provision for law enforcement to conduct 'arrests' via video calls or online monitoring. If you receive such calls, it is a clear scam. In fact, recently enacted new criminal laws do not provide for any provision for law enforcement agencies conducting a digital arrest. The law only provides for service of the summons and the proceedings in an electronic mode.[3]

[2] Sunainaa Chadha, No one can arrest you through video calls: Digital arrest fraud on the rise, https://www.business-standard.com/finance/personal-finance/digital-arrest-fraud-explained-atomic-energy-employee-duped-of-rs-71-lakh-124100700305_1.html

[3] Ibid.

(A) Recent Cases:

- Recently in November, a Dubai-based entrepreneur was put under digital arrest at Bhopal for several hours. The fraudsters posed themselves as officials from the Telecom Regulatory Authority of India (TRAI), the Central Bureau of Investigation (CBI) and the Mumbai Cyber Crime Branch. They subjected him to hours of questioning to gather his personal, sensitive and banking information. Fraudsters informed him that many fraudulent bank accounts had been opened using his Aadhar Card. In this case, Mr. Oberoi was terrified by the incident and meanwhile, one of his friends who came to visit him got to know about it and based on suspicion he reported the incident to cyber police. The cyber police immediately swung into action and a team was dispatched to the location. While Mr. Oberoi was being interrogated by the accused persons the cyber police team intervened and asked the scammers to show proof of identity and they abruptly cut that video call.

- Another instance was highlighted recently, it is also the longest digital detention case in India reported till now. In this case, a 77 year old lady from South Mumbai was targeted by fraudsters and kept under digital detention for more than a month. The accused duped her of 3.8 crore rupees and posed themselves as Mumbai Police officials. She first received a WhatsApp call where she was told that the parcel that she sent to Taiwan had been stopped which contained five passports, a bank card, 4KG clothes, MDMA drugs etc., to which she denied sending any parcel to anyone. Then she was told her Aadhar card details were used in crime. She was then asked to download Skype where Mumbai Police officials would interrogate her. There several fraudsters pretending themselves to be police officials ordered her not to cut the call, sought her bank account details and asked her to transfer money into the bank account given by them and also sent her a notice with a fake crime branch logo. They told her if they found money to be clear they would return it to her. She was also asked to continue the 24X7 video call with them. Over some time she transferred 3.8 crore rupee to them, but when she didn’t get back her money she suspected them and somehow managed to talk to her daughter about it and she asked her to approach to police. The police then freezed the accounts of fraudsters.

- In one of the largest individual cyber fraud cases registered in Pune, a 59 year old senior IT executive lost 6.29 crore rupee to fraudsters posing themselves as CBI officers. They threatened him with the allegation that his connection was found in a money laundering case and thereby he was ordered to be under their surveillance and was also arrested digitally. Since November 9 for more than a week, he was under digital arrest. On the pretext of interrogation all the information as to his details, bank accounts and properties were sought by fraudsters and then at different times they asked him to transfer different sums of money in several accounts. When he mentioned this to his family members he realized that he had become a victim of cyber fraud and lodged an FIR with Pune police.

- Another incident took place in Gwalior city of Madhya Pradesh on November 7 where a software engineer became a victim of this offence. The victim was threatened that she would be arrested for the offence of sending drugs via parcel and an investigation is going on regarding it. The fraudster pretended then connected her call to another one who himself to be a police official and was told that some illegal activities were going on via her bank account, under this fear and mental pressure of 9 hours of digital arrest her private information like her Aadhar card and PAN card photos and her bank account details were taken from her and made her transfer 6 lakh rupees to different accounts of the scammers. And then tried to take load into her name but till then she suspected them and lodged a complaint against them.
- On the 8th of October, victim advocate Jagmohan Shrivastava also faced the same circumstances, where on a call he was told that a parcel had been booked to Beijing using his Aadhar Card details. The parcel contained MDMA drugs and 12 debit cards were seized by the customs department. Fraudsters digitally arrested the victim from noon to night and told him that he had been also found guilty in a money laundering case and later connected him to a fake CBI officer who told him that more than 2 dozen cases were pending on him. During the arrest, they got his old account closed and got him a new account opened with 16 lakh rupees and made him transfer it to them.
- Another incident took place in Khandwa (Madhya Pradesh) where a nurse employed in a district medical college was arrested digitally for a continuous span of 21 hours and wasn’t even allowed to go out of sight of the camera to drink water. She continuously sits in front of the camera from 2 PM to 11 AM of next day. She got a fake call where fraudsters pretended to be from the Maharashtra Crime Branch and informed that her name was involved as a drug peddler in a case and hence arrested. She was also ordered to share screenshots of her every call. When her friend came to meet her they also threatened her with the same allegations and in fact, she gave 50000 rupees. Somehow her friend managed to tell the incident to her neighbour and hence they intimated the

police and saved both of them from further being looted.

- A 25-year-old IIT Bombay student also fell victim to a digital arrest scam in which he lost 7.29 lakh rupees. The incident started in July when he got a call from fraudsters who posed as a TRAI officer, informing him that his mobile number had been linked to illegal activities and 17 complaints were pending regarding it. They told him that he had to obtain a no-objection certificate from the police to prevent his number from being deactivated and transferred the call to a person who appeared as a police officer. He alleged the student was involved in a money laundering case and asked about his Aadhar card details. He then threatened that student to transfer 29,500 rupees to avoid arrest. The fraudster also informed him that he was under digital arrest and could not contact anyone. The next day they again demanded money and the student shared his bank account details with them, which allowed the fraudsters to withdraw 7 lakh rupees from his account and assured him he wouldn't face arrest now. When the student searched the digital arrest online he realized that he had been scammed and hence filed a police complaint.
- The most highlighted case of digital arrest was of the **head of the Vardhman group**, and the most audacious part of the scam was that the fraudsters set up a virtual courtroom where a man impersonating the then **Chief Justice of India, Dr. D.Y. Chandrachud** presided over his case. The fraudsters posed themselves as Central Bureau of Investigation (CBI) officials and told him that an account had been opened using his Aadhar card details and had been involved in suspicious transactions. They further claimed that his identity had been misused and that the account was tied to several accounts facing ongoing investigation. He was also sent a fake arrest warrant bearing stamps of the Enforcement Directorate (ED) and Mumbai police. During the video call, he was shown a fake court order with the court's emblem, bar code and digital signature, which closely resembled those used in real court orders, directing him to deposit Rupees 7 crore into different bank accounts. Later the order was sent to him via WhatsApp and believing that his identity had been misused and that he was under investigation he deposited the amount into those bank accounts.
- Another incident took place in Noida where a 50 year old women became victim of digital arrest. The fraudsters used the identity of an IPS officer and the founder of an Airline service and posed them as law enforcement officials alleged the victim was involved in a money laundering case and told her that a SIM card registered in her name

had been used for fraudulent activities in Mumbai. Then they transferred the call to another fraudster posing as a Mumbai police official, who investigated her and arrested her via video call on Skype for more than 10 hours and it ended up when she transferred around 11.11 lakh rupees to them.

- A 23 year old girl from Faridabad got a call from a fraudster posing as a Lucknow customs officer who told her that a package was being shipped from India to Cambodia containing many bank cards and passports associated with her Aadhar card number. She was further told that in an ongoing investigation, she was found to be a part of a group of people involved in human trafficking. Her call was then transferred to another fraudster posing as a CBI official who told her that she was being digitally arrested till she paid 5 per cent of the total amount of money laundering as a penalty and she ended up transferring Rupees 2.5 lakh to a bank account shared by fraudsters.

The background of these cases shows that in most of the cases, the accused persons have some sort of personal information about their targets and their major focus is on the people who are entrepreneurs, businessmen or wealthy people so that they can demand huge amounts of money from them. But this does not mean they can’t target middle-class people in several cases they have also become victims. Recently, incidents also occurred with the people who are living alone and are working personnel. Generally, people become victims in two scenarios, one is they fear being involved in crime and face penal consequences and the other is that they are unaware of the latest crimes in society. This is because either they are not in touch with the news or ignorant towards the laws. Regarding the rise in incidents in Madhya Pradesh, an advisory has been issued by the police department stating that in India there is no such law that can empower police to arrest digitally and all such calls are fake. The people who know this offence must spread awareness in society and recently an SBI staff saved a senior citizen from fraud of digital arrest. This scam is rising because in each case these criminals terrify the victims in such a way that they believe their details are used in the offence and to escape from punishment deposit the demanded amount in accounts provided by the criminals.

IV. Data and observations

As many as 7.4 lakh complaints were received between January 1 and April 30 this year, while 15.56 lakh complaints were received in 2023, according to the National Cybercrime Reporting Portal (NCRP) data as reported by Indian Express. As many as 9.66 lakh complaints were reported in 2022, up from 4.52 lakh in 2021.[4]

A survey has been conducted over 900 people categorized into 3 age groups i.e. below 25, 25 to 50 and above 50 having 300 people in each group. The survey was conducted in a close-ended questionnaire form. It was conducted in an inductive reasoning method where from particular observations general results are concluded. Most questions were in yes or no format and it contained questions like:

1. Have you heard about the digital arrest?
2. Is it legal in India?
3. Have you ever been the victim of digital arrest?
4. Do you know any victims of digital arrest personally?
5. Is there any law in India which deals with digital arrest?
6. Are present laws enough to deal with it?
7. Have you made efforts to spread awareness about it?
8. How do you know about it by not applicable/newspaper/online?

(A) Result:

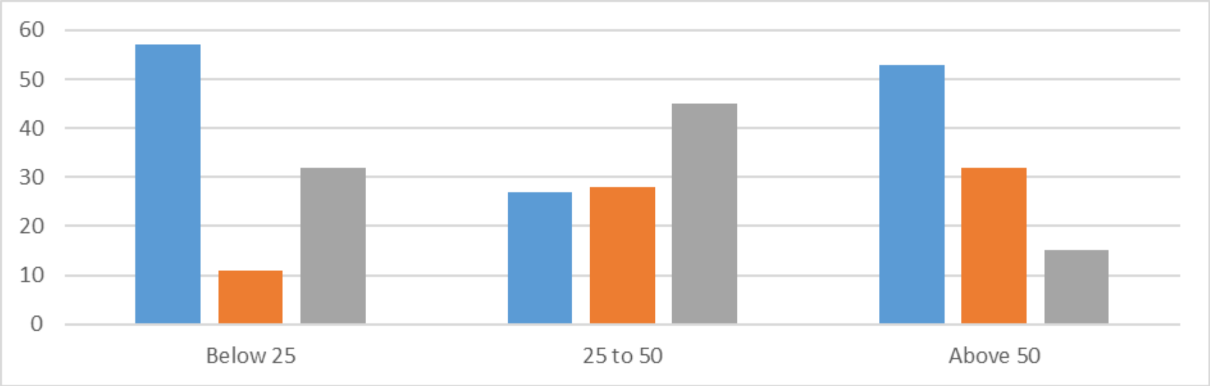
In the below 25-year age group, the survey has been conducted on people above 16 to keep data relevant. The data given below is in percentage form.

Question	**BELOW 25**		**25 TO 50**		**ABOVE 50**	
Number	**YES**	**NO**	**YES**	**NO**	**YES**	**NO**
1	40	60	72	28	33	67
2	50	50	33	67	58	42
3	7	93	21	79	22	78
4	5	95	48	52	29	71
5	30	70	61	39	56	44
6	57	43	49	51	68	32

[4] Indians lost ₹120 cr in digital arrest frauds in Jan-April quarter this year: Report, https://www.livemint.com/news/indians-lost-120-cr-in-digital-arrest-frauds-in-jan-april-quarter-this-year-report-11730078842257.html

7	13	87	28	72	10	90

The data as to question number 7 below shows answers between 3 choices. First one shows that this question is not applicable on them as they don't know about it. Second one shows that how much people got to know about it through newspaper and third one shows how much of them became aware through online mode. It is as follows:



(B) Observations:

On considering the above data it can be concluded that both young age and old age people are potentially vulnerable towards this offence it has also been observed that among them also above 20 are more aware but few of the people above 23 have also become victims of the offence. It has been seen in middle-aged people that they are quite aware about it and are more aware because tech-savvy. People above 50 are also less aware about its legality or illegality. People aged between 25-50 and above 50 are somehow equally seen to be victims of the offence. People between 25 to 50 have a wide circle hence seen to be more in touch of victims of digital arrest. People themselves are seen less aware about the offence and very few among them spread awareness regarding it. Among them second age group is seen quite active in spreading news about it.

V. Legal framework for protection against digital arrest

In India, with changes in technology legal system has also adapted gradually, to deal with digital crimes. As digital arrest has risen recently, there is no particular law on it but primary laws which can govern digital arrest include:

- Information and Technology Act, 2000: It is the foundation of India's cyber law and covers many cyber offences. It empowers agencies to investigate, arrest and prosecute offenders. Section 66 deals with offences like data theft and unauthorized access and provides punishment up to 3 years or a fine up to 5 lakh rupees or both. Section 66-C deals with the offence of identity theft and can cover the fraudsters who use monograms, seals or signatures of authorities to commit this scam. It is punishable with imprisonment up to 3 years and a fine which may extend to 1 lakh rupees. Section 66-D deals with the offence of cheating by personation using computer resources and is liable with the same punishment as Section 66-C. the fraudsters personate as CBI, ED or any other law enforcement officials and so are liable under this section. Section 67, 67-A and 67-B deal with offence related to obscene content. Sometimes the fraudsters transmit obscene content to victims and then threaten them by telling them that they are found guilty of keeping, publishing or transmitting such sexual content or that they are found involved in human trafficking. Section 69 Grants the government power to intercept, monitor or decrypt information in cases involving national security or cyber terrorism and this offence is against national security. The provisions of this act apply to offences committed from out of India targeting any computer resource located in India. Recently this has been found that many fraudsters call from outside the country. Section 70-B empowers the central government to appoint an agency named as Indian Computer Emergency Response Team to serve as a national agency to perform functions like collection and analysis of data, forecast alerts about cyber offences, handling the incidents and so on. This agency can intercept communication on mobile networks, emails or social media platforms and is very useful in cases of cyber terrorism and organized crimes.

- Bhartiya Nyaya Sanhita (BNS) formerly known as Indian Penal Code (IPC) provides some provisions which can apply to digital crimes. Section 111 of BNS deals with organized crimes and their punishment. It involves continuing any unlawful activity including cyber-crimes either singly or jointly. It also covers organized crime syndicates. Section 204 BNS (IPC 170) deals with the punishment for personating a public servant. Section 351(4) BNS (IPC 507) deals with criminal intimidation by anonymous communication and making demands of money which these fraudsters generally do.
- The Bhartiya Nagarik Suraksha Sanhita (BNSS) formerly known as The Criminal Procedure Code provides guidelines for arrest and it also applies to cases involving digital offences. Under this sanhita law enforcement agencies can confiscate electronic devices, freeze bank accounts or block access to social media accounts as part of an investigation but there is no provision for digital arrest in any procedure under the sanhita.

- Digital forensics technology is used by law enforcement agencies to collect, analyse and preserve electronic evidence and this technology is also used to track IP addresses and decrypting communication on encrypted platforms.
- Online surveillance technologies like geo-fencing and real-time monitoring help authorities identify and track suspected criminals. Social media platforms like Telegram, Facebook, Whatsapp, Instagram, Skype etc. have become hotspots for illegal activities and financial fraud. These surveillance agencies use artificial intelligence and machine learning tools to track suspicious activity on social media.
- Law enforcement agencies use blockchain analytics tools to track and trace illicit transactions. Blockchain's stability assures that once digital evidence is recorded, it cannot be modified or erased. No single part has control over it. This feature safeguards the integrity of the evidence and ensures that it remains tamper-proof and admissible in proceedings.

VI. Treaties and international law that assure fundamental right of privacy at online platforms

Article 12 of the Universal Declaration of Human Rights provides that no *one shall be subjected to arbitrary interference and intrusion with his privacy. Every person has the right to immunity against interference or attacks and has the right to protection of the law against such attacks.* Article 17 of the International Covenant on Civil and Political Rights also provides that no one shall be subjected to arbitrary or unlawful interference with his privacy nor to unlawful attacks on his honour. These rights also provide the same level of protection on online platforms. Since 2013, the UN General Assembly and Human Rights Council have adopted numerous resolutions on the right to privacy in the digital age. The resolution on the right to privacy in the digital age was adopted by the Human Rights Council in September 2019 and again in December 2020.

The International Covenant on Civil and Political Rights (ICCPR), the Universal Declaration of Human Rights, the WIPO Internet Treaties etc. require countries to provide legal protection against online offences infringing the privacy of individuals. It requires countries to prohibit the deliberate alteration or deletion of electronic records and information. General Data Protection Regulation (GDPR) is also one of the regulations to protect people and entities from online frauds.

The United Nations Convention against Transnational Organized Crime, also known as the **Palermo Convention**, obligates the state to enact domestic criminal offences legislation to target organized criminal groups and to adopt new frameworks for legal assistance, extradition and cooperation in law enforcement. **Convention on Cybercrime,** also known as the **Budapest Convention**, is the first international agreement aimed at reducing cybercrime by harmonizing laws, improving investigating techniques and increasing international cooperation.

India also has its own data protection laws and recently enacted The Digital Personal Data Protection Act, 2023. It aims to regulate data processing and give citizens control over their personal information. Apart from this Information and Technology Act 2000 and Bhartiya Nyaya Sanhita 2023 also deals with certain kinds of cyber offences.

(A) Challenges Faced by Law Enforcement Agencies:

The major challenge faced by law enforcement agencies is that most fraudulent calls are made via technology named IP telephony, commonly known as Voice over Internet Protocol (VoPI). It allows users to make voice calls over the internet (VoIP) through messaging apps such as WhatsApp instead of using traditional phone calls. This complicates the tracing of calls as servers are sometimes outside India. Obtaining data from these platforms is both challenging and time-consuming for these agencies. Moreover, the rapid increase in such cases makes it difficult for police and other agencies to respond quickly. Due to such delay in taking appropriate actions, money defrauded from victims is transferred to multiple accounts or converted into cryptocurrency.

(B) **Steps taken by the government to combat digital arrest:**

The government has blocked more than 1000 fraudulent Skype accounts which were linked with blackmailing, extortion and offences like digital arrest. Moreover, several SIM cards, mobile devices and mule accounts used by fraudsters have also been blocked recently. All this is done under blockchain technology which means to stop further activity by such fraudulent accounts and connected accounts. Several alerts and awareness programs have been run on social media platforms like ‘cyberdost’ and others. Other than this networking companies also send SMS time to time to their customers regarding such cyber frauds. A helpline number 1930 has also been issued by the government and whoever receives any such call may immediately report the incident on the helpline number or on the website of the National Cyber Crime Reporting Portal. The Ministry of Home Affairs in March 2024, issued a press release, alerting people against incidents of digital arrest by cybercriminals.

Ministry of Home Affairs has identified cross-border crime syndicates which are part of larger organised crime and run a vast economic crime network. Indian Cybercrime Coordination

Centre established by the Ministry of Home Affairs provides a framework to deal with cross-border digital crime syndicates. Its main aim is to curb cyber offences in the country by proposing amendments to cyber laws to match up rapidly evolving technologies.

The government of India has entered into a bilateral agreement (MLAT), which implemented Mutual Legal Assistance Treaties (MLAT) with other countries for cybercrimes to allow the exchange of information and evidence to enforce laws and to deter such cybercrimes. In May 2024, a committee comprising various law enforcement and intelligence agencies was established to address the transnational cybercrimes targeting Indians.

On 27th of November PIB Delhi issued a press release To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, newspaper advertisement on digital arrest scam, announcement in Delhi metros on digital arrest and other modus operandi of cyber criminals, use of social media influencers to create special posts on digital arrest, digital displays on railway stations and airports across, etc.[5]

(C) Suggestions:

It is crucial to be aware of the tactics used by cybercriminals for the commission of offence of digital arrest. Some of the major suggestions to combat this offence are:

- **Beware of Spoofed Numbers:** Offenders use technology to make their phone numbers appear likely to be of government agencies or law enforcement officials. The government must spread awareness as to the illegality of such calls on behalf of any government agency. It must be spread through online and offline modes that government agencies never make such calls. If a person receives any suspicious call pretending through a law enforcement agency and demanding money or trying to make an online arrest a person may either hang up the call and try to contact with relevant agency or department to verify the authenticity of such call and must also file a complaint providing relevant information to cybercrime department in concerned area.
- **Be Cautious of Urgent Demands:** Scammers create a sense of urgency in their target

[5] CASES OF DIGITAL ARREST SCAMS, https://pib.gov.in/PressReleasePage.aspx?PRID=2077948

to pressurise them to transfer funds to them. Victims are asked to make immediate payment to keep any matter or information as confidential, here to protect themselves they must be cautious that there is a possibility of it being a scam. People must be cautious that legitimate authorities never ask for personal or financial information over the phone calls or through text messages. In neither circumstance, anyone should provide their personal or financial details to any stranger. Scammers often use obtained information to steal their identity or access their bank accounts. If anyone is threatened with imprisonment unless they pay a certain sum of money, they must think about it as this is a clear indication that they are being scammed.

- **Beware of Social Media Scams:** Scammers use social media platforms to target potential victims. They send corrupt messages or links to their target. People must be cautious of unauthorised messages through unknown individuals and must not click such links from unauthorised messages.
- **Spreading awareness:** The government must conduct awareness programs to spread awareness about the scams and techniques used by cybercriminals to extort money from victims. Awareness programs must be conducted to stay updated on emerging threats. Victims must also raise awareness about digital arrest scams by sharing information with their friends and family.
- **Seek Legal Advice:** Anyone who believes themselves to be a victim of digital arrest must if possible seek advice from legal experts as to their position regarding digital arrest and its validity.
- **Report Suspicious Activity:** On being unsure about the authenticity of any call or message people must try to verify the information through the proper channel of government. If anyone notices suspicious activity on their accounts or receives any suspicious messages or emails they must report it to the local police or cybercrime helpline number or National helpline Number 1930 and can also file a complaint on the National cyber-crime reporting portal.

VII. Conclusion

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 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 people need to be proactive and aware. Recently due to spreading awareness, there comes many bold examples of people who don't fall in the grip of these criminals and set up an example for society.

A two-factor authentication and frequent change in the password can lower the risk of unauthorized access to accounts. One must be aware of phishing and protect their devices with reliable antiviruses to enhance privacy. To protect one from digital arrest, citizens must know about this constantly changing cyber threat with collective knowledge, and educated practices, and legislature must enact strong cyber security laws. As it is also a cross-border crime syndicate so in most of the cases the fraudsters call through SIM cards registered outside India. It is known that the code of India is +91 so people must generally avoid picking up such calls to prevent themselves from falling into the grip of this offence.

*****