INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

UNDERSTANDING OF DIGITAL ARREST: DEFINITION, METHODS AND IMPLICATIONS

AUTHORED BY - ASMITA MALLICK
7th Semester, BA LLB Heritage Law College

CO-AUTHOR - PRITHWISH GANGULI, ADVOCATE
LLM (CU), MA in Criminology and Forensic Sc (NALSAR), MA in Sociology (SRU)

Synopsis:

Digital arrest represents a novel and alarming form of cybercrime, where individuals or organizations find their digital rights and access unlawfully restricted, effectively creating a state of virtual detention. Unlike traditional cybercrimes, digital arrest focuses on the unauthorized seizure of digital assets, access to networks, or online presence, often through malicious software, ransomware, or unauthorized control over digital systems. This emerging threat not only challenges existing cybersecurity frameworks but also exposes significant gaps in legal protections, as current laws may not adequately address the nuances of such a crime. The research will explore the concept of digital arrest in depth, analyzing its mechanisms, the legal implications for victims, and the broader impact on privacy and digital freedom. By examining case studies and current legal responses, the paper aims to provide a comprehensive understanding of digital arrest and propose necessary reforms to better equip legal and cybersecurity systems to combat this growing threat.

Keywords:

Digital Arrest, Cyber Crime, Cyber Law, Cyber Security, Unauthorized Detention.

Introduction:

"Digital Arrest" is a new scam where **authorities stop or control online data and communications to catch or prevent illegal activities like hacking or cybercrimes**. The victims are forced to stay on video calls with the scammers until their demands are met. The scammers pose as officials and extort money from unsuspecting citizens over video calls. Criminals are extorting money in exchange for agreeing not to expose the false legal cases that

 ISSN: 2582-6433

have been constructed. This helps in investigating and stopping online criminal activities. Digital arrest" isn't a standard legal or technical term. In legal contexts, "arrest" typically refers to the physical detention of a person by law enforcement. However, digital arrests made connection with cybercrimes, such as hacking, identity theft, or online fraud. These arrests often involve the identification and apprehension of suspects who commit crimes using digital means.

Cyber police from four different states, including the national capital, have reported around four such cases in the past seven months. Decode spoke with cyber police from Haryana, Uttar Pradesh, and cyber experts to understand what this "digital arrest" means and the tactics employed by scammers in this new scam.

Meaning:

Digital arrest is a new kind of cybercrime where the fraudsters typically call a potential victim and inform that the victim has sent or is the intended recipient of a parcel, which contains illegal goods, drugs, fake passports or any other contraband item. Sometimes, they also inform the near or close one of the victims has been found to be involved in a crime or an accident and is in their custody. A demand for money is made to compromise by the scammers. In certain instances, unsuspecting victims are made to undergo "Digital Arrest" and remain visually available over Skype or other video conferencing platform to the fraudsters, till their demands are fulfilled. The fraudsters are known to use studios modeled on Police Stations and Government offices and wear uniforms to appear genuine. Restrictions or controls imposed on individuals' digital access or communications is a kind of a digital house arrest.

Sharade Kamalanathan and Dr. Rakhi R Wadhwani explained "Digital Arrest" as a method of cybercrime, involves individuals posing as law enforcement officers to intimidate and coerce victims into transferring significant sums of money.

Procedure/Methods:

- In these scams, scammers pose as law enforcement authorities, including police or customs agents. They trick people into thinking that they are about to be digitally arrested for spurious legal offenses.
- These fraudsters typically call a potential victim and inform that the victim has sent or

 ISSN: 2582-6433

is the intended recipient of a parcel, which contains illegal goods, drugs, fake passports or any other contraband item.

- Sometimes, they also contact the relatives and close friends of the victim who has been found to be involved in a crime or an accident and is in their custody. Even the cybercriminals are hypnotizing people who find themselves "digitally arrested" for days.
- The fraudsters are known to use studios modeled on Police Stations and Government offices and wear uniforms to appear genuine.
- Scammers are now impersonating local law enforcement authorities and threatening victims to have arrested on false accusations.
- A demand for money is made to compromise the "case".
- In a panic, the victims attempt to settle the lawsuit and wind up having to pay the amount. The offenders incite panic and a sense of urgency by using digital communication tools such as video calls and messaging.
- They also manipulate victims by using threatening language, fabricating proof, and demanding large sums of money in order to escape any legal repercussions.
- In certain instances, unsuspecting victims are made to undergo "Digital Arrest" and remain visually available over Skype or other video conferencing platform to the fraudsters, till their demands are met.
- Recently, a 23-year-old Faridabad residential woman was the victim of a recent fraud. She lost Rs 2.5 lakh to hackers posing as customs agents. In the case the victim was forced to believe that she was a part of a passport trafficking case and she would have to pay Rs 15 lakh to keep herself from being placed under "digital arrest." She ultimately paid Rs 2.5 lakh to resolve the matter. Throughout the encounter, the scammers advised her not to log out of Skype.

Cases:

- Scammers held a woman from Noida, under 'digital arrest' over a Skype call for an entire day by pretending to be cops. As a result, they took amount of Rs 11 lakhs from her.

On the morning of November 13, the woman received a call from the scammer who identified as a police officer from Mumbai. Reetu Yadav, in-charge of cyber crime police station Noida sector 36, where the woman eventually filed a complaint, narrated to Decode on how the events

 ISSN: 2582-6433

unfolded. The scammer told the woman that her Aadhaar card had been used to buy a SIM card, which is connected to a money laundering case in Mumbai. They told her that an arrest warrant had been issued in her name and convinced the woman to transfer all her savings to an ICICI bank account. She was even forced to apply for a loan of Rs 3 lakhs to make the total payment of Rs 11 lakhs. Officer Yadav told Decode that the woman didn't even realize she had been scammed for a day. "She told us that at first she was afraid to share what had transpired and only days later realized she had fallen victim to an elaborate online scam," Yadav said.

According to the police, the scammer first called the woman on her phone and later asked her to join a Skype call with a man who identified himself as an IPS officer. "He conveyed to her that she was under interrogation for alleged involvement in certain crimes, including money laundering, as they had linked her to," the officer said. Over a Skype call, the scammers not only frightened that woman with the money laundering case but claimed that an arrest warrant was issued against her. Fabricated documents were presented to her via Skype.

According to the victim, she noticed a setup resembling a proper police station in the background, adorned with photos of India's freedom fighters on the walls, accompanied by the distant sounds of wireless communication.

Throughout the session, the scammers insisted on her silence and constant online presence. She was ensured not to share this information with anyone or disconnect the call, citing 'national security' as the reason, implying potential repercussions. This purported senior officer questioned her for nearly half an hour, the police told Decode. They told her that they found 246 debit cards, belonging to the prime accused, the founder of the airline, at his residence. To her shock, one of these cards bore the name of the Noida woman and had been utilized to open a bank account using her Aadhaar card. The fraudsters played the next trick by telling her that she seemed to be innocent in the case. However, to aid the investigation, she was directed to transfer funds and then if they found no involvement of her, her money would be returned.

In the end, to give her a false sense of assurance regarding her innocence, they coerced her into virtually signing several fake documents under the pretext of validating the investigation.

 ISSN: 2582-6433

Real-Life Cases:

In India:

- **Rohini's Experience:** Rohini, 50-years old woman, received a phone call from individuals claiming to be "TRAI officials." They informed her that a SIM card registered with her Aadhaar card which had been involved in money laundering activities. The scammers manipulated her for transferring her entire savings, amounting to Rs 11,11,295, into a specified account.
- **Retired IAS Officer Incident:** In another case, a retired IAS officer had faced a scam by individuals posing as officers from the Mumbai Police Crime Branch. The officer suffered a financial loss of Rs 11.5 lakh as a result of this fraudulent activity which is named as digital arrest.
- **IT Professional's Digital Arrest:** A 32 years old IT professional became the target of a sophisticated digital arrest scam. The perpetrators impersonated as legal officials and subjected the individual to a "digital arrest" lasting for seven hours. Throughout this period, the victim was defrauded of Rs 3.75 lakh.

In Other Countries:

Here are some recent notable cases involving digital arrests in other countries:

- **United States v. Ganias**: In this case, the retention of digital files outside the scope of a warrant where the Second Circuit Court stated that the government's retention of files from lawfully imaged hard drives for over two and a half years violated by the Fourth Amendment.
- **Global Organized Crime Sting (2021)**: In a massive operation, the FBI and Australian law enforcement developed and operated an encrypted device company called ANOM. This allowed them to infiltrate organized crime networks in over 100 countries, leading to hundreds of arrests worldwide.
- **Cybercriminal Arrest in Estonia (2021)**: A cybercriminal named Maksim Berezan was apprehended in Latvia and extradited to the United States. He pleaded guilty to conspiracy to commit wire fraud and other cybercrimes, highlighting international cooperation in tackling digital crimes.

 ISSN: 2582-6433

Digital Arrest Scams: Legal Implications

Digital arrest scams are often involving multiple collaborators which can result in serious legal consequences.

- **Criminal Offenses:** Perpetrators of digital arrest commit criminal offenses such as fraud, extortion, and impersonation. These actions are punishable under relevant sections of the law.
- **Impersonation:** Impersonating a police officer or government official is a serious offense. In many jurisdictions, it is a crime to falsely represent oneself as a law enforcement officer.
- **Extortion:** Scammers use fear tactics to extract money from victims. Extortion is a criminal act, and those involved can face imprisonment and fines.
- **Money Laundering:** Victims are often coerced into transferring funds to designated accounts. If the scammers are successful, they may be involved in money laundering, which is illegal.
- **Conspiracy:** Conspirators in these scams may face charges of conspiracy to commit fraud or related offenses.
- **Civil Liability:** Victims who suffer financial losses can pursue civil claims against the perpetrators, potentially leading to compensation awards.
- **International Jurisdiction:** As these schemes can cross borders, international law enforcement collaboration is crucial in tracking down and prosecuting offenders.

The legal consequences vary by jurisdiction. If you suspect a digital arrest scam, promptly report it to local authorities. As cybercriminals continue to evolve their tactics, it's crucial for individuals to stay informed and take necessary precautions to safeguard finances and personal information. Before encountering suspicious calls or messages, always verify the authenticity before taking any action. Vigilance and awareness are essential in preventing such incidents and to protect themselves from financial and legal consequences.

To avoid falling for such cybercrime:

The following are certain best practices for ensuring the same:

- **Remain vigilant and observant:** Recognize typical fraudster techniques and schemes, such as digital arrest scams.

 ISSN: 2582-6433

- **Always confirm who is calling**: Scammers exploit fear and urgency to manipulate individuals. If someone calls you posing as a law enforcement official, get their official identification documents and contact details to confirm their identity.
- **Remain composed and raise doubts about the veracity of the circumstances:** Legitimate legal issues are usually resolved by official processes rather than by sudden dangers. If one receives calls from unknown numbers claiming to be law enforcement officials, exercise caution. Do not provide personal information or make any payments without verifying their identity. Contact your local police station or the relevant authorities to confirm the legitimacy of the call.
- **Never expose personal information:** Legitimate law enforcement agencies do not demand money over the phone. If anyone asks you to transfer funds urgently, be aware and verify their credentials thoroughly. Refrain from disclosing money or personal information (particularly your bank account information) without proper verification to unidentified or unreliable people.
- **Always verify assertions again and get supporting documentation:** Verify facts on legal allegations on your own. Confirm the veracity of any accusations by getting in touch with the appropriate legal or law enforcement bodies in your area via proper methods.
- **Report Incidents:** If you suspect that you are being targeted by a digital arrest scam, report it to the police immediately. Prompt action can help prevent further financial losses and protect others from falling victim to these scams.
- **Use only official channels for communication:** Only official channels are used by law enforcement organizations that are legitimate. When in doubt, use the publicly accessible contact details to independently get in touch with the appropriate agency.
- **Stay informed**: Learn the main warning signs of scammers, which include demands for money over the phone, threats of urgent legal action, and unusual ways of payment.

Measures to Protect Yourself from Digital Arrest Scams:

Sustaining a practical and observant approach toward cyber security is the key to lowering the peril of being targeted and experiencing digital arrest.

- **Cyber Hygiene:** It means maintaining cyber hygiene by regularly updating passwords, software. It also includes enabling two-factor authentications to reduce the chances of unauthorized access.

 ISSN: 2582-6433

- **Phishing Attempts:** These can be evaded by refraining from clicking on dubious links or downloading attachments from unknown sources and also authenticating the legitimacy of emails and messages before sharing any personal information.
- **Secured devices:** By installing reputable antivirus and anti-malware solutions and keeping operating systems and applications up to date with the latest security protocols.
- **Security Measures:** Use robust security settings on communication platforms. Avoid sharing personal information or financial details over the phone or online without verifying the request's legitimacy.
- **Virtual Private Networks (VPNs):** VPNs can be employed to encrypt internet connections thus enhancing privacy and security. However one must be cautious of free VPN services and OTP only for trustworthy providers.
- **Educational Resources:** Follow "14C's Cyberdost" on social media (Twitter, Face book, Instagram) for Info graphics, Videos, and updates on cybercrime prevention. Regularly update one on the latest cybercrime trends and protection strategies.
- **Monitor online services:** A regular review of online accounts for any unauthorized or unlawful activities and setting up alerts for any changes to account settings or login attempts may help in the early detection of cybercrime and coping with it.
- **Secure communication channels:** Using secure communication techniques such as encryption can be done for the protection of sensitive information. Sharing of passwords and other information must be cautiously done especially in public forums.
- **Awareness:** The increasing prevalence of cybercrime known as "digital arrest" underscores the need for preventive measures and increased public awareness. Educational initiatives that draw attention to prevalent cyber threats—especially those that include law enforcement impersonation—can enable people to identify and fend off scams of this kind. The collaboration of law enforcement agencies and telecommunication companies can effectively limit the access points used by fraudsters by identifying and blocking susceptible calls.

Ministry of Home Affairs has issued an alert against incidents of 'Blackmail' and 'Digital Arrest' by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies to extort money from unsuspecting victims.

The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, coordinates activities related to combating cybercrime in the country. MHA is closely working

 ISSN: 2582-6433

with government officials for identifying and investigating the cases.

The **Indian Cybercrime Coordination Centre (I4C)** has collaborated with Microsoft and actively combating this organised online economic crime. I4C has also blocked more than 1,000 Skype IDs involved in such activities. The MHA has identified that these scams are operated by cross-border crime syndicates, making them part of a larger, organized online economic crime network.

It is also facilitating blocking of SIM cards, Mobile devices and Mule accounts used by such fraudsters. I4C has also issued various alerts through info graphics and videos on its social media platform **'Cyberdost'** for e.g.- Face book, Instagram and others.

Indian Cybercrime Coordination Centre (I4C)

- It was established in New Delhi to provide a framework and eco-system for **Law Enforcement Agencies (LEAs) for dealing with Cybercrime** in a coordinated and comprehensive manner.
- I4C is working towards its vision to create an **effective framework** and ecosystem for prevention, detection, investigation, and prosecution of cybercrime.
- I4C aims to strengthen the capabilities of law enforcement agencies (LEAs) and **improve coordination among various stakeholders** and LEAs.
- I4C is envisaged to act as the **nodal point to curb Cybercrime in the country.**
- It proposes **amendments to cyber laws to keep up with rapidly evolving technologies** and international cooperation.
- **Mutual Legal Assistance Treaties (MLAT)** is a bilateral agreement between two or more countries that allows for the exchange of information and evidence to enforce criminal or public laws. The implementation of MLAT with other countries for consultation with the relevant authority in MHA.

How remote access software is used in the 'digital arrest' scam?

According to Delhi's Cyber Police crime record, there has been a significant surge in cyber fraud cases, with over 25,000 cases filed till August this year. This marks a substantial 212% increase compared to the 8,000 cases reported during the same period last year. These cases encompass a variety of frauds, including UPI fraud, bank scams, and email scams, resulting in

 ISSN: 2582-6433

a financial loss exceeding Rs 200 core this year in Delhi.

In 2022, cybercrime cases surged by 24.4%, as per recent National Crime Records Bureau (NCRB) data. Karnataka, Telangana, and Maharashtra, relatively affluent states, contributed over half of these cases.

Shubham Singh who is a cyber security expert closely collaborating with government cyber investigation agencies, explained that scammers employ various tactics to induce fear in victims. It includes making false accusations and divulging personal information such as Aadhaar details or the name of their bank account. He also explained about the scammers leverage the threat of legal action and immediate arrest to coerce victims into settling the matter through financial means.

"They strategically isolate victims to gain control: They might deceive individuals into installing remote access software like any desk or Team Viewer on their devices. This grants the scammers control over the victims' online activities, enabling them to monitor actions and pilfer sensitive information," Shubham Singh elaborated.

Conclusion:

The rapid advancement of technology in modern society poses significant challenges to law enforcement agencies worldwide, particularly in combating cybercrime. In this context, digital arrests have emerged as a critical tool in the fight against online offenses such as hacking, identity theft, and other unlawful activities. While the term "digital arrest" is not universally defined, it generally refers to the complex interplay between legal authority, technological capability, and individual rights in the digital age.

One troubling manifestation of digital arrest involves cybercriminals impersonating law enforcement officers to commit fraud. These criminals deceive their victims by claiming they are involved in illegal activities and demand payment to avoid arrest. Typically, they allege that the victim has sent or received parcels containing illegal items, such as drugs or contraband. The fraudsters often use fake identities or doctored images of police personnel to bolster their credibility, insisting that the victim must pay to resolve the matter. In some cases, victims are coerced into staying on video calls to ensure compliance until the criminals' demands are met.

 ISSN: 2582-6433

A growing number of complaints are being reported on the National Cyber Crime Reporting Portal (NCRP) regarding threats, blackmail, extortion, and "digital arrests" carried out by cybercriminals posing as authorities from the police, Central Bureau of Investigation (CBI), Narcotics Department, Reserve Bank of India (RBI), Enforcement Directorate, and other law enforcement agencies. Across the country, many individuals have fallen victim to these schemes, losing substantial amounts of money. This type of crime is highly organized, often orchestrated by cross-border syndicates engaged in economic fraud.

In certain countries, the concept of digital arrest may also refer to legal restrictions on individuals' online activities, such as internet shutdowns or surveillance of digital behaviour by law enforcement or intelligence agencies. To counteract these fraudulent activities, governments are increasing public awareness, urging citizens to remain vigilant, and encouraging them to report suspicious incidents through cybercrime helplines or official websites.

Bibliography:

1. https://www.cyberpeace.org/resources/blogs/digital-arrest-fraud: 03/08/2024
   https://www.msspalert.com/native/digital-arrests-the-new-frontier-of-cybercrime: 05/08/2024
2. https://pib.gov.in/PressReleasePage.aspx?PRID=2020570: 10/08/2024
3. https://www.drishtiias.com/daily-updates/daily-news-analysis/digital-arrest-scams: 14/08/2024
4. https://www.the420.in/all-you-need-to-know-about-digital-arrest-a-novel-cybercrime-trend/: 15/08/2024