DIGITAL ARREST SCAMS AND PROCEDURAL SAFEGUARDS UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023: A CRITICAL ANALYSIS

Tanishq Balaji Alandkar, BA.LL.B., Manikchand Pahade Law College, Chh. Sambhajinagar, Maharashtra, India.

ABSTRACT

Rapid growth of Information Technology and E Commerce has transformed the modern Era. In today's modernize era with the advent of internet and information technology one peculiar specimen stands out as its sophisticated evolution i.e. Digital Arrest. The term Digital Arrest has not been explicitly defined anywhere however we can understand the term Digital arrest as 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. The scammers typically conduct intimidation via digital platforms and display fake FIRs and claim money transfer in the name of settlement of dispute. Victims are coerced into transferring money or disclosing sensitive information under threats of legal action. Cases span across India as of mid-2026, cyber cells have busted multiple gangs in Delhi, Bengaluru, Chennai, Hyderabad, etc., seizing mobiles and freezing account. The enactment of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, a legislative overhaul intended to replace the CrPC, incorporates technology-oriented reforms intended to improve efficiency and transparency. This paper critically analyses digital arrest scams in India, and whether the BNSS provides adequate procedural safeguards to address digital arrest scams in India.

Keywords: Digital Arrest, Cyber Crimes, BNSS, Cyber Crimes.

DIGITAL ARREST SCAMS AND PROCEDURAL SAFEGUARDS UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023: A CRITICAL ANALYSIS

INTRODUCTION:

The Digital Transformation of India has significantly increased the wide spread use of internet and E Governance. As every coin has two sides while these developments have enhanced accessibility it has also facilitated new forms of Cyber Crime. Digital Arrest occupies as one of the most eminent Cyber Frauds of present times. A foundational point every citizen must know that there is no concept of Digital Arrest in Indian Law. The introduction of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), was intended to modernize criminal procedure and facilitate technology-based investigation and prosecution. The paper critically analyses the Digital Arrest Scams and Procedural Safeguards under the Bharatiya Nagarik Suraksha Sanhita, 2023. It seeks to evaluate whether the BNSS provides adequate safeguard against Digital Arrest or merely embodies general principles.

OBJECTIVES OF THE PAPER:

- To examine the nature and operation of digital arrest scams in India.
- To analyze procedural safeguards available under BNSS, 2023
- To evaluate the effectiveness of BNSS provisions in combating cyber fraud.
- To identify legal gaps and practical challenges in implementation.
- To propose reforms for strengthening protection against digital arrest scams

RESEARCH METHODOLOGY

This paper follows a doctrinal legal research methodology, relying primarily on Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Nyaya Sanhita, 2023, and the Information Technology Act, 2000. Secondary sources include journal articles, government reports, judicial decisions, and scholarly commentaries relating to cybercrime and criminal procedure.

UNDERSTANDING DIGITAL ARREST

Digital arrest is a type of scam in which the perpetrator represents or impersonates himself as a government Enforcement Officer and falsely accuses the victim or layman of having committed a crime in the nature of Money Laundering, or tax evasion. The scammers typically induces the person in the trap and thereby extorts money in the name of settlement of dispute. The perpetrator further showcases false FIRs, Fake Arrest Warrants, Forged Documents etc. The Digital Arrest scammers prohibit the victim from contacting any other person. Since many people are unaware that the Arrest in India can only be conducted physically and according to procedure prescribed by laws the scammer take an advantage of the same and attack innocent individuals.

MODUS OPERANDI OF SCAMMERS

Digital arrest scams follow a carefully orchestrated sequence designed to maximise panic, isolation, and financial extraction.

1. **Initial Contact:** Scammers pose as law enforcement or government officials — CBI, ED, Customs, Interpol, RBI — via phone calls, emails, WhatsApp messages, or fake official letters. The first contact appears routine: a parcel notification, a KYC update request, or a tax verification query.

2. **Creating Panic:** The victim is falsely accused of serious crimes such as money laundering or drug trafficking and threatened with immediate arrest, manufacturing a state of fear that impairs rational thinking.

3. **Digital Verification:** To add credibility, scammers send fake documents, doctored arrest warrants, or fabricated court orders, and may conduct video calls dressed as police officers against official-looking backdrops.

4. **Isolation and Coercion:** Victims are instructed not to inform family, friends, or lawyers, and may be kept on continuous video calls — a form of "digital custody" — for hours or even days.

5. **Payment Demand:** Victims are coerced into paying a "security deposit" or "fine" via UPI, cryptocurrency, prepaid gift cards, or through real-time surveillance of banking credentials.

6. **Disappearance and Money Laundering:** Once the money is transferred, scammers

vanish. Funds are divided into smaller amounts, funneled through multiple mule accounts, and transferred offshore — making recovery virtually impossible.[1]

LEGAL FRAMEWORKS ADDRESSING DIGITAL ARRESTS:

The Cyber Crime of Digital Arrest is not an explicitly recognized offence under the Criminal Laws in India, however various provision of the Bhartiya Nyaya Sanhita 2023 and the Information Technology Act 2000 come into play when such acts are committed. The key provision of that come into play when such act is committed are as follows:

1. **Impersonating a Public Servant**: Punishable with imprisonment of six months to three years, along with a fine.[2]

2. **Cheating:** Punishable with imprisonment of up to seven years and a fine.[3]

3. **Forgery**: Punishable with imprisonment of up to seven years and may incur a fine[4].

4. **Extortion:** Punishable with imprisonment of up to ten years and may incur a fine[5].

5. **Identity Theft:** Punishable with imprisonment of up to three years and a fine of up to ₹1 lakh[6].

6. **Cheating by Personation Using Computer Resources**: Punishable with imprisonment of up to three years and a fine of up to ₹1 lakh.[7]

PROCEDURAL SAFEGUARDS UNDER BNSS:

The Rajasthan High Court has taken *suo moto* cognizance of the issue[8]. Justice Anoop Kumar Dhand has reiterated that there is no concept of "digital arrest" under the Bharatiya Nagrik Suraksha Sanhita, 2023 ("**BNSS**"). The High Court has also directed the Government to raise

[1] https://www.drishtijudiciary.com/to-the-point/bharatiya-nyaya-sanhita-&-indian-penal-code/digital-arrest-the-modern-day-cyber-scam
[2] Section 204 of BNS
[3] Section 318 of BNS
[4] Section 336 / 336(3) of BNS
[5] Section 308 of BNS
[6] Section 66C of IT Act
[7] Section 66D of IT Act
[8] In Re: In the matter of tackling the issue of 'Digital Arrest Scams', Cyber Crimes and saving the innocent people from losing their money and lives, Rajasthan High Court (2025).

awareness and the Reserve Bank of India to take steps to halt payments made to such fraudsters.

Under the Bhartiya Nagrik Suraksha Sanhita 2023, there is no concept of Digital Arrest. However the BNSS the provides some adequate safeguards which are as follows:

1. Section 173 the BNSS permits electronic communication and digital filing of information relating to offences. Victims of cybercrime can more easily approach law enforcement authorities through electronic platforms

2. Under Section 63 the BNSS allows for Electronic Service of Summons, however each such summon must be encrypted, bear the image and seal of the Court, and bear a digital signature.

3. Additionally, a notice under Section 35(3) of the BNSS directs individuals suspected of committing a cognizable offence to appear before the police for requisite questioning, if their arrest is not mandated in accordance with Section 35(1) of the BNSS.

4. The BNSS recognizes the growing importance of electronic evidence and supports the use of technological tools during investigation. Proper preservation and authentication of electronic evidence are crucial for successful prosecution.

CHALLENGES IN ADDRESSING DIGITAL ARREST SCAMS:

Some of the key challenges associated with Digital Arrest Scams are as follows:

1. Jurisdictional Issues: Cyber Crimes operate across the state and national boundaries. Determination of Jurisdiction in investigation is a significant challenge.

2. Lack of Specific Legislation: The existing legal framework lacks provision relating to digital arrest which creates a legislative lacuna. This has created a gap in addressing the rise of Cyber Crimes.

3. Lack of Awareness: Many citizens are unaware of the procedural laws relating to Arrest which gives a benefit to the Cyber Scammers. Old person become the primary victim of Digital Arrest.

4. Evidentiary Issues: One of the major challenge in Digital Arrest Scams is collecting the Evidence. The Crime committed is totally in digital form and it is inherently required to collect

all the calls, videos, chats, messages etc. All the Evidence need to be certified under Section 63 of Bhartiya Sakshya Adhiniyam to prove its credibility and authenticity.

5. Delay in Recovery: The funds obtained through the scam are distributed by the offenders on different banks accounts. It creates a challenge to recover the money.

CONSTITUTIONAL DIMENSIONS

Article 21 which is the cornerstone of all the Fundamental Rights violated in the pretext of Digital Arrest. The Sacrosanct Right of Privacy guaranteed under Article 21 is also violated as the scammers directly breach the privacy of individual in name of investigation procedure. Apart from this the Principles of Natural Justice and Due process is also violated. Public awareness of these Rights can significantly reduce the threat of Digital Arrest.

COMPARATIVE ANALYSIS

UNITED KINGDOM:

Commonly referred as “Courier Fraud” or impersonation scams. The victims are told that their bank accounts are taken into custody and are under investigation. To protect the money they are told to transfer it to other account.

Legal Measures: Specialized cybercrime units investigate technology-enabled fraud. The Fraud Act 2006 and Computer misuse Act 1990 provide legal backing.

UNITED STATES:

These scams are commonly referred as “Imposter Scams”. The victims are contacted and told that their social security number is linked to crime like drug trafficking and tax evasion. They are then coerced to transfer money in form of Gift cards or Crypto currency.

Legal Measures: The Federal Bureau of Investigation regularly issue public advisories regarding impersonation scams. Extensive cooperation exists between law enforcement agencies and financial institutions.

RECOMMENDATIONS:

1. Legislative Measures

- Enact a section in BNS criminalizing "fraudulent impersonation of public authority causing harm" with enhanced penalty.
- Establish a proper procedure under the BNSS.
- Require all court or police notices (summons, warrants, notices) to carry a verifiable digital signature or QR code linking to an official portal.
- Enact rules via the IT Act or BNSS making malicious deep fake/video impersonation of officials a distinct offence when used to defraud.

2. Institutional Reforms

- Strengthen Cyber Crime Cells in each state with digital forensic tools and training on deepfake analysis.
- Create specialized cybercrime investigation units.
- Enhance training programs for investigators and prosecutors.

3. Public Awareness

- Nationwide awareness campaigns explaining lawful arrest procedures.
- Public advisories regarding common cyber fraud techniques.
- Integration of cyber safety education into academic curricula

CONCLUSION:

Digital arrest scams represent a serious challenge to India's evolving digital ecosystem. These offences exploit technological tools, psychological manipulation, and public ignorance of legal procedures. The Bharatiya Nagarik Suraksha Sanhita, 2023 introduces important reforms aimed at modernizing criminal procedure and integrating technology into investigation and prosecution processes. The BNSS provides a useful procedural framework through electronic reporting, forensic integration, and enhanced transparency measures. Nevertheless, significant gaps remain in enforcement capacity, public awareness, and cybercrime-specific protections.

Addressing digital arrest scams requires a multidimensional approach combining legislative reform, institutional strengthening, technological innovation, and public education. Ultimately, the success of BNSS in combating cyber-enabled fraud will depend not merely upon statutory provisions but upon their effective implementation and the state's ability to adapt continuously to emerging technological threats.