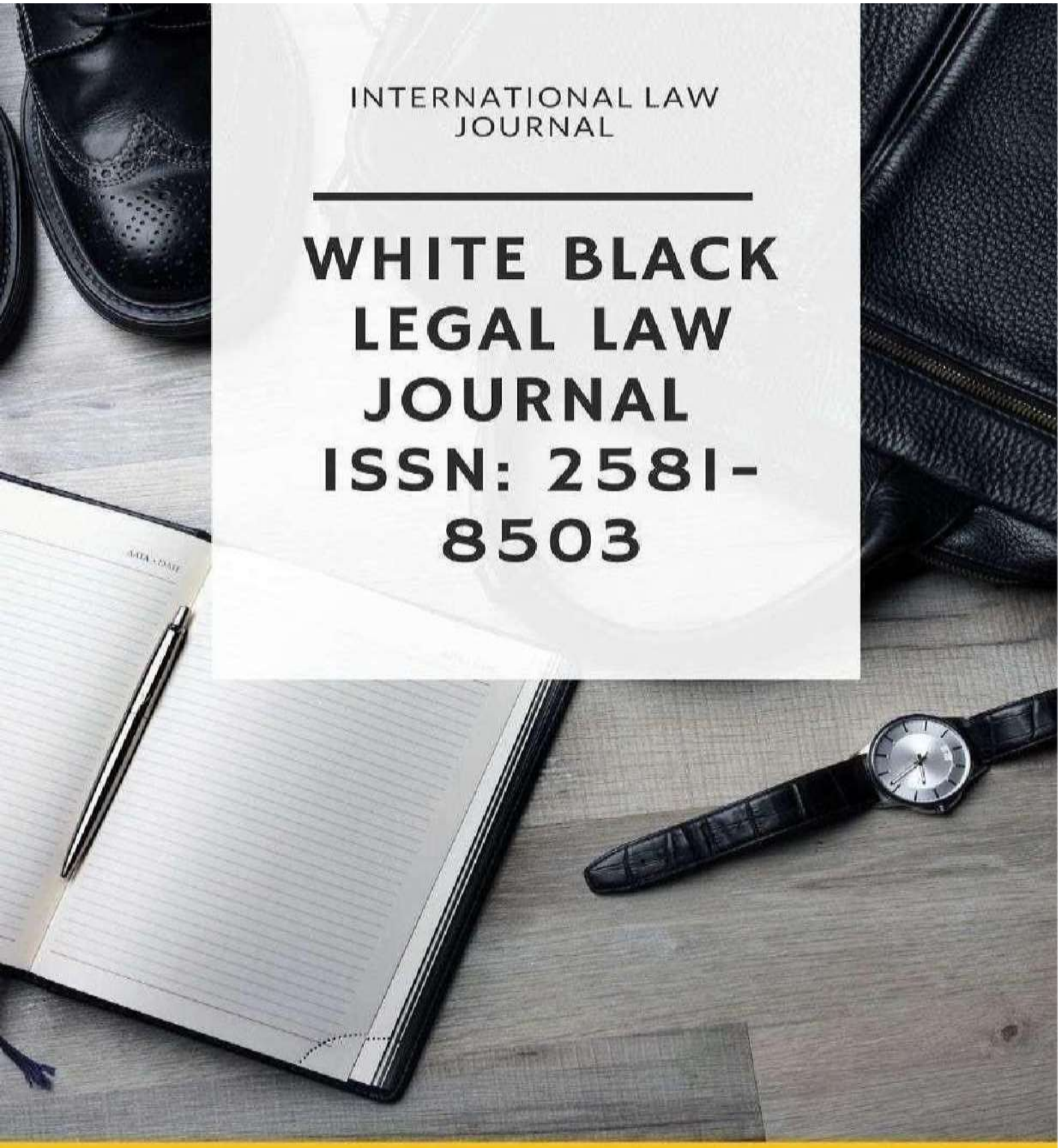

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 2 | 5th June 2025 ISSN: 2581-8503

FROM FIRS TO FAKES: UNPACKING THE LEGALITY AND THREAT OF DIGITAL ARREST IN INDIA

AUTHORED BY - NEHA
Research Scholar
Maharishi Markandeshwar Deemed To Be University, Mullana, Ambala

Abstract

Digital arrest is a fraudulent illusion whereby victims are coerced via video calls, impersonated documents, and psychological manipulation into believing they are under arrest. This doctrinal study critically examines the legal framework, modus operandi, judicial responses, and remedies available in India. It argues that although India lacks statutory recognition for digital arrest, the existing legal regime — including the BNS/CrPC and IT Act — provides the tools to prosecute perpetrators under impersonation, cheating, data theft, and intimidation. Recommendations include legislative amendments, greater public awareness, and cyber-investigation enhancement.

Keywords: Digital arrest; cyber fraud; impersonation; IT Act 2000; Bharat-iya Nyaya Sanhita; doctrinal method; video-call scams

Introduction

The digital world, once hailed as humanity's greatest leap into the future, has become a double-edged sword. As innovations in artificial intelligence, deepfake technology, and encrypted communication flourish, they also give rise to novel and insidious forms of crime. Among these is the phenomenon of "Digital Arrest"—a cyber-enabled scam where individuals are coerced into believing they have been virtually arrested by law enforcement agencies for alleged crimes such as money laundering, drug trafficking, or illegal financial transfers. This pseudo-legal theatre is enacted through video calls, forged notices, and impersonated officers—often bolstered by cloned voices and doctored documents—to trap victims in a psychological lockdown until they either surrender sensitive data or make financial transfers.

This research undertakes a doctrinal investigation into the emergence, legal context, and

implications of digital arrest in India. It explores how this crime—still not clearly defined or codified in Indian law—has rapidly evolved into one of the most psychologically disturbing and economically devastating cyber frauds of recent times.

Origin and Global Emergence

The earliest precursors of digital arrest scams were observed in China around 2019, where fraudsters began impersonating police officials over internet calls to extort money from unsuspecting citizens. According to Interpol and reports from Chinese cybercrime monitoring agencies, such calls were often made from overseas call centers based in Cambodia, Laos, or even parts of Eastern Europe. These criminals relied on sophisticated techniques—spoofed caller IDs, uniforms worn on video calls, background visuals mimicking government offices, and doctored documents—to manipulate and psychologically trap victims.The victims were often told that their identity was linked to a criminal case, and to "avoid arrest," they must remain online at all times, isolate themselves, and comply with verbal interrogation—sometimes for hours or even days. The practice came to be colloquially referred to as "digital detention" or "virtual kidnapping" in global law enforcement circles.Singapore also became a hotspot around 2020–21. There, the government issued multiple warnings through its police and financial institutions after dozens of citizens fell prey to similar scams. Victims often transferred large sums of money to foreign bank accounts in panic, believing the calls to be real due to the remarkably convincing visuals and mannerisms of the imposters.

Entry into India

India first began to experience early tremors of this cybercrime model around 2022, but the phenomenon exploded in 2023–2024, largely due to the rapid digitization of services, widespread use of mobile internet, and a significant trust deficit among the public when dealing with official authorities. The nature of Indian society—with its bureaucratic complexity, fear of law enforcement, and digital illiteracy in vulnerable populations—made it fertile ground for the flourishing of this scam. Initial reports emerged from metropolitan cities like Bengaluru, Delhi, Mumbai, and Kolkata, where upper-middle-class individuals, senior citizens, and professionals were duped of lakhs, sometimes crores, of rupees. In many cases, the impersonators claimed to be from reputed agencies like the Narcotics Control Bureau, Customs, Cyber Police, or even the Supreme Court of India, complete with fake emails, forged signatures, and judicial-style video conferencing. By mid-2024, the Indian Cyber Crime

Coordination Centre (I4C) had begun to identify a trend. They reported a staggering rise in complaints where victims were made to stay on Skype, WhatsApp, or Google Meet calls for several hours or even multiple days, being interrogated, threatened, and manipulated until they made financial transactions "in lieu of bail" or "verification." In most cases, the entire psychological game was so well-orchestrated that victims did not even realize it was a scam until much later. According to I4C data, between January and April 2024, over ₹120 crore was lost to digital arrest scams. In total, over 7.4 lakh complaints were registered in 2024 across India, with many experts estimating the real numbers to be much higher due to unreported cases. A Reddit user, through open-source analysis, pegged the figure closer to ₹1,935 crore, indicating a financial pandemic that has largely remained under-documented.

Present Status in India

Despite the alarming rise in cases, India still lacks a specific statutory definition or framework that acknowledges "digital arrest" as a recognized crime. As of 2025, such scams are being prosecuted under a patchwork of laws—primarily under provisions related to cheating (Section 420 IPC/BNS), identity theft (Section 66C IT Act), forgery, impersonation, criminal intimidation, and extortion. In some cases, Section 72A of the IT Act (breach of privacy) and the Digital Personal Data Protection Act, 2023 have been invoked when data misuse is involved. However, due to the novelty and complexity of these crimes, coupled with cross-border jurisdictional hurdles (many call centers are located in Cambodia, Myanmar, etc.), law enforcement agencies have struggled to effectively trace and prosecute perpetrators. The landmark moment came in July 2025, when a West Bengal court convicted nine accused in India's first digital arrest case, sentencing them to life imprisonment for defrauding a retired scientist of over ₹1 crore. The court termed their acts as "economic terrorism", underscoring the psychological and financial trauma caused. This judgment has since become a symbolic victory for cybercrime prosecution in India, yet it remains an isolated case in a sea of growing fraud. On the institutional front, the government has made efforts to curb this menace. The Ministry of Home Affairs, through I4C, has begun blocking WhatsApp/Skype IDs, launching public awareness campaigns, and promoting its helpline 1930. States like Maharashtra are issuing digital police ID cards with QR verification to prevent impersonation, and cities like Mysuru have launched door-to-door campaigns to educate the elderly. However, these are still reactive and fragmented efforts, and the absence of a national legislative framework continues to allow these scams to proliferate.

Concept of Digital Arrest

The term "Digital Arrest" is not a statutory term recognized in Indian legislation. It is, however, an emergent cybercrime phenomenon that blends psychological manipulation with digital impersonation to extort, defame, or defraud individuals. At its core, digital arrest refers to the fraudulent simulation of a legal arrest by impersonating law enforcement or judicial authorities via online platforms, typically involving video calls, fake documentation, and coercive tactics designed to manipulate the victim into submission. The illusion created is so compelling that victims are often convinced they are under investigation or immediate threat of imprisonment.

The modus operandi of such scams follows a specific pattern. Typically, the victim receives a phone or video call from someone impersonating a police officer, customs officer, or even a judge. These imposters use spoofed caller IDs, professional-sounding language, and even deepfake technologies to recreate the likeness of government officials. Victims are shown forged arrest warrants, customs seizure notices, or fake FIRs bearing their name. In many instances, they are told their Aadhaar, PAN, or bank account is linked to criminal activity — often international money laundering or narcotics trade — and they must cooperate to "avoid arrest." What follows is a coercive and prolonged interrogation conducted entirely online, during which the victim is isolated — instructed to stay on video calls, avoid contacting family, and obey the caller's orders under the threat of imminent arrest. This digital confinement—while lacking any real legal authority—is made psychologically convincing through intimidation, manipulation, and fear of public humiliation. Victims are eventually persuaded to transfer money, share sensitive information, or provide remote access to their devices.

Unlike traditional scams which rely solely on financial bait, digital arrest preys on psychological vulnerability, particularly the fear of authority. It capitalizes on public unawareness of digital rights, procedural safeguards in criminal law, and the inability of many to distinguish between genuine and fake official communications. Importantly, a digital arrest has no legal basis in Indian law. Under the Code of Criminal Procedure (CrPC) or its contemporary replacement, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, an arrest must be carried out by a legally authorized officer, either with a valid warrant or under permissible grounds. There exists no provision for arrest through video call or WhatsApp message. Thus, digital arrest is not merely a scam — it is a gross impersonation of the justice system, carrying deep legal and ethical implications.

Legal Framework in India

The phenomenon of digital arrest, though alarming in scale and impact, currently exists within a grey area of Indian law. It has no specific statutory recognition, yet it is not without remedy. Various general and special laws, including the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Information Technology Act, 2000, contain provisions that can be invoked to prosecute the perpetrators of such frauds. A doctrinal analysis reveals that while the offence of digital arrest is technologically modern, the tools to address it legally already exist—albeit in a fragmented, interpretative manner.

1. Bharatiya Nyaya Sanhita, 2023 (BNS)

The BNS, which replaces the Indian Penal Code, 1860, retains and modernizes several classic offences that are frequently invoked in cases of digital arrest. These include:

Section 316 (Cheating): This provision deals with dishonest or fraudulent inducement to deliver property or to consent to retain property. In digital arrest scams, victims are typically forced to transfer money under the false belief of avoiding arrest, falling squarely within the definition of cheating.

Section 319 (Personation and Impersonation): Digital arrest scams often involve fraudsters pretending to be police officers, customs officials, or even judges. Section 319 criminalizes impersonation with the intent to deceive or to obtain a benefit—whether financial or otherwise.

Section 336 (Forgery of Documents or Electronic Records): Most digital arrest operations involve fake letters, warrants, and seizure notices that appear to be issued by legitimate agencies. This section criminalizes the creation and use of forged electronic records.

Section 356 (Criminal Intimidation): Threatening a person with harm, arrest, or legal action to extort money or compel compliance is a textbook case of criminal intimidation under BNS.

Section 357 (Anonymous Communication for Intimidation): This provision, relevant for impersonated calls using unknown or spoofed numbers, can be used where the identity of the caller is hidden but used to threaten the victim. Together, these provisions make it possible for law enforcement agencies to file FIRs and initiate criminal proceedings against cyber fraudsters operating digital arrest schemes. However, the enforcement still requires a well-trained cybercrime apparatus to trace, identify, and prosecute such digital offenders, many of whom operate from beyond Indian borders.

2. Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)

The BNSS, which substitutes the Criminal Procedure Code (CrPC), governs the procedures for arrest, investigation, and prosecution. A key argument in the legal invalidity of digital arrest lies in the procedural safeguards enshrined in this code.

Section 35 BNSS (Arrest with or without Warrant): It prescribes who may arrest, when arrest is permissible, and under what circumstances. Nowhere does the law authorize arrest via a phone or video call. Therefore, any "digital arrest" is by nature illegal and unconstitutional.

Section 36 (Notice of Appearance before a Police Officer): This section outlines the formal way an individual can be summoned by police. Digital arrest scams, where people are ordered to "stay online" without any proper summons, violate this provision.

Section 38 (Rights of Arrested Persons): It mandates that an arrested person must be informed of the grounds of arrest and of their right to bail. In a digital arrest scenario, these constitutional protections are entirely absent, making such practices not just unlawful but violative of Article 21 of the Constitution of India. The BNSS also reinforces the importance of due process, something flagrantly absent in these scams. Thus, when scammers attempt to fabricate legal proceedings over digital mediums, they directly contravene the procedural and constitutional mandates of Indian criminal jurisprudence.

3. Information Technology Act, 2000

The IT Act, being India's principal law governing cyberspace, plays a critical role in prosecuting digital arrest frauds. Several sections of the Act are frequently invoked in such cases:

Section 66C (Identity Theft): This section penalizes the use of another person's identification information—such as Aadhaar, PAN, or official designations—for fraudulent purposes. Impersonating a police officer or judge digitally is a violation of this provision.

Section 66D (Cheating by Personation Using Computer Resource): Specifically targets impersonation scams conducted via computers or communication devices. Digital arrest scams, by virtue of their digital medium and impersonation tactics, fall squarely under this provision.

Section 67 and 67A: Although originally meant to prevent the circulation of obscene material,

these sections have been invoked where scammers use explicit threats or doctored images/videos to blackmail victims during a digital arrest.

Section 72A (Breach of Confidentiality and Privacy): When personal information accessed during the scam is misused, this provision can be triggered, especially if the fraudsters access financial accounts, bank statements, or other private data under coercion.

Thus, while the IT Act does not define "digital arrest," it provides ample legal ammunition to criminalize its components — impersonation, intimidation, data theft, fraud, and privacy invasion.

4. Digital Personal Data Protection Act, 2023

This recently enacted legislation enhances protections around personal data, particularly consent and usage of sensitive digital information. In digital arrest cases, scammers often coerce access to mobile devices, bank accounts, and government-linked IDs, making unauthorized use or processing of such data a direct violation of this law. Under Section 7 of the DPDP Act, data fiduciaries must process personal data only for lawful purposes, with informed consent. Digital arrest scams flagrantly violate these conditions by obtaining consent under fear or misinformation, thus making them liable under this Act as well.

5. Right to Privacy and Article 21 of the Constitution

The Supreme Court of India, in K.S. Puttaswamy v. Union of India (2017), declared the right to privacy as a fundamental right under Article 21. Digital arrest scams—by detaining people psychologically, surveilling them via video calls, and manipulating personal information—constitute an assault on this fundamental right. Such actions, though perpetrated by private individuals, indirectly undermine public trust in state institutions. The doctrinal implication here is that state inaction in preventing such scams or educating citizens could be viewed as a failure of the constitutional obligation to protect fundamental rights.

6. Jurisdiction and Enforcement Challenges

Digital arrest crimes often originate from overseas call centers, especially in regions like Myanmar, Cambodia, or Eastern Europe. This presents a jurisdictional challenge under both substantive and procedural law. Section 75 of the IT Act provides for extraterritorial jurisdiction, allowing India to prosecute offences committed outside India if the computer

system affected is located within India. However, enforcement depends on mutual legal assistance treaties (MLATs), INTERPOL red corner notices, and regional cyber-cooperation frameworks — many of which are slow and underdeveloped.

Gaps and Challenges in Addressing Digital Arrest in India

The phenomenon of digital arrest represents a rapidly escalating cyber threat that not only exploits technological loopholes but also manipulates legal ignorance and psychological vulnerability. While Indian laws—especially under the Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and Information Technology Act, 2000—offer tools to combat various aspects of this scam, the enforcement ecosystem is riddled with structural and operational shortcomings. These gaps reflect deeper challenges: legislative ambiguity, jurisdictional difficulties, technological manipulation, under-resourced enforcement, and public unawareness. This section critically evaluates these gaps and challenges through a doctrinal lens and examines how the legal system, despite its foundational strengths, remains outpaced by the sophistication and agility of digital offenders.

1. Absence of Statutory Recognition and Definition

One of the foremost doctrinal deficiencies is the absence of a statutory definition or recognition of "digital arrest" in Indian law. Unlike offences such as cheating, extortion, and identity theft—which are clearly outlined in the BNS and IT Act—digital arrest operates as a composite crime. It is a fusion of impersonation, coercion, psychological manipulation, and digital misrepresentation. However, because no standalone provision categorizes or defines it, enforcement remains dependent on a piecemeal invocation of overlapping sections. This results in confusion at the First Information Report (FIR) stage, where police often fail to identify which offences have been committed. For instance, a victim may report impersonation and intimidation via video call, but unless the investigating officer is cyber-trained, it may be misclassified as a general cheating case. The lack of definitional clarity leads to delays, dilution of charges, and legal loopholes during prosecution.

2. Fragmented Legal Response and Interpretative Burden

Although multiple legal provisions are available—under BNS, IT Act, DPDP Act, and IPC (for older cases)—they must be interpreted contextually to suit each scam's unique modus operandi. This places a heavy interpretative burden on courts and law enforcement, particularly in rural or semi-urban jurisdictions where cybercrime awareness remains low. For example, Section

66D of the IT Act covers impersonation using digital resources, and Section 316 of the BNS deals with cheating. But the connection between a fake video call simulating a Supreme Court hearing and "cheating" is not always apparent to lower judiciary or field-level officers. The lack of standard legal templates or investigative SOPs (Standard Operating Procedures) leaves room for wide discretion, leading to uneven enforcement and frequent case dismissals.

3. Jurisdictional and Enforcement Difficulties

One of the most complex challenges in tackling digital arrest scams is jurisdictional enforcement. A vast majority of these scams are operated from foreign soil—often from organized criminal rackets in Cambodia, Myanmar, Thailand, and Eastern Europe. In many cases, the perpetrators are not Indian nationals or operate from countries with which India has no effective Mutual Legal Assistance Treaty (MLAT).

While Section 75 of the IT Act permits extraterritorial application of Indian law when a computer system located in India is affected, its real-world application remains symbolic rather than effective. Cross-border investigations are extremely slow, bureaucratic, and diplomatically sensitive. Even if the Indian authorities succeed in tracing the origin of a call, extradition and prosecution remain near-impossible without bilateral cybercrime treaties, which are currently lacking with many of these countries.Furthermore, Indian cybercrime cells often lack dedicated personnel or linguistic and technological capabilities to track and collaborate with foreign agencies on real-time digital evidence collection.

4. Deepfake Technology and Evidentiary Challenges

Digital arrest scams increasingly employ AI-generated voices, synthetic avatars, and deepfake video simulations to create convincing impersonations of government officials. Fraudsters can now mimic the voice and facial expressions of real judges, police officers, or celebrities using publicly available software. This presents profound challenges for evidence gathering and admissibility in court. Indian courts and police forces are still evolving in their understanding of digital forensics, especially in relation to AI-generated evidence. Without expert digital forensic validation, such evidence can be dismissed or considered inconclusive. There is also no formal legal test under Indian law for deepfake detection. While the Indian Evidence Act allows for electronic records under Section 65B, it lacks updated guidance on synthetic media. As a result, both prosecution and defence face considerable difficulties in proving the authenticity or forgery of digital evidence presented in digital arrest cases.

5. Institutional Capacity and Cyber Infrastructure Deficits

India's cybercrime infrastructure, though expanding, remains disproportionately under-resourced relative to the scale of emerging threats. Many police stations still lack trained cybercrime officers, and even major cities often rely on a handful of experts for digital forensics.

Additionally, there is a disconnect between central and state cyber authorities. While bodies like the Indian Cybercrime Coordination Centre (I4C) and Cyber Dost issue advisories, the enforcement and case handling is state-dependent, and suffers from bureaucratic delays, overlapping jurisdictions, and lack of data sharing. The cyber helpline 1930 is functional but often overburdened. In several cases, victims report delays of hours—sometimes days—before intervention, by which time the money has already been transferred and withdrawn by mules in foreign accounts.

6. Public Unawareness and Social Engineering Exploits

Perhaps the most glaring and under-addressed challenge is public ignorance. Digital arrest scams succeed largely because they prey on fear of authority and ignorance of legal procedures. Many citizens are unaware that: Arrests cannot be conducted over video calls.

Police officers cannot demand payment or bank details for investigation. Judicial hearings or summons are not served via Whatsapp or Skype. Scammers exploit this ignorance using social engineering tactics—they apply pressure, use legal jargon, display fake IDs or letterheads, and demand confidentiality. Victims, particularly senior citizens, professionals, and women living alone, are isolated psychologically and manipulated into compliance. Awareness campaigns run by Cyber Dost and police departments in cities like Mysuru and Mumbai are commendable, but they remain sporadic and urban-centric. There is an urgent need for a nationwide, multilingual awareness programme, embedded even into school syllabi and community outreach programs.

7. Psychological and Societal Trauma: The Invisible Harm

Digital arrest scams inflict a kind of harm that goes beyond financial loss—they psychologically paralyze victims, some of whom suffer post-traumatic stress, anxiety, depression, and even suicidal ideation. The Bengaluru man who ended his life after losing ₹13 lakh is a tragic testament to the intensity of such trauma.

However, there is no formal psychological or legal rehabilitation mechanism for such victims. The legal system treats these cases as financial fraud, while the psychological coercion and emotional damage are rarely addressed or compensated. There is no provision for counselling, state compensation, or mental health referrals post-victimization—an omission that weakens India's restorative justice framework.

Conclusion

The rise of "Digital Arrest" in India is emblematic of the seismic shifts occurring at the intersection of law, technology, and criminal psychology. What initially appeared as isolated incidents of cyber fraud has now emerged as a full-fledged, organized criminal enterprise operating across national borders, leveraging the power of AI, deepfakes, and digital impersonation to exploit fear, authority, and ignorance. As this research has shown, the Indian legal framework—despite its evolution through the Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), and the Information Technology Act, 2000—remains largely reactive and fragmented when it comes to combating such nuanced, multi-layered cybercrimes. The term "digital arrest" does not exist in statutory language, yet its impact is undeniably real. People across the country are being coerced into financial, emotional, and psychological submission by criminals masquerading as legal and law enforcement authorities. These scams simulate the theatre of legality—judicial summons, investigation notices, custodial threats—all through phone calls, video conferencing, and fake documentation. The result is a terrifying psychological trap where the victim is manipulated into parting with money or personal data under the illusion of state sanction. It is a new kind of virtual incarceration—one that leaves no marks on the body, only bruises on the psyche. A deeper examination reveals that this phenomenon thrives in the legal grey zones between existing statutory provisions. Laws like Section 66D of the IT Act (punishing impersonation using computer resources), Section 316 of the BNS (cheating), and Section 503 and 507 (criminal intimidation and anonymous threats) are invoked in such cases. However, these are disjointed provisions that lack the specificity and coordination needed to comprehensively address the layered mechanics of digital arrest. The absence of a clear legal definition, dedicated offence category, or procedural roadmap severely undermines the capacity of law enforcement to act swiftly and decisively.

Moreover, the doctrinal application of these laws is marred by interpretative inconsistencies.

Police personnel often lack cyber training, courts face delays due to evidence admissibility challenges, and jurisdictional issues—especially in cases involving foreign operators—make investigation and prosecution nearly impossible. In practice, the burden of proof falls heavily on the victim, who must first convince the authorities that a crime has even occurred. This represents a complete inversion of justice, where the victim is met with disbelief while the scamster walks away freely. A particularly disturbing facet of this issue is the psychological warfare waged by the perpetrators. These are not mere scams; they are orchestrated acts of emotional manipulation, often executed with military precision. Victims are isolated, threatened, coerced, and gaslighted into silence. The emotional toll is profound, yet the legal system offers no counselling, compensation, or rehabilitative support for victims. The Indian state's response remains transactional—focused on the financial loss rather than the emotional trauma or the breach of dignity and trust. The gaps are not only legal but also institutional. While India has set up cybercrime cells and helpline numbers like 1930, the actual response mechanism is riddled with infrastructural deficits—understaffed cyber units, lack of technical expertise, absence of forensic tools for AI-based fraud detection, and no real-time cross-border intelligence sharing. The fragmented coordination between the Centre and the States further delays actionable response. The Indian Cybercrime Coordination Centre (I4C) and initiatives like Cyber Dost are steps in the right direction, but they are insufficient in scale, inconsistent in reach, and urban-centric in design. Rural and semi-urban populations remain dangerously vulnerable.

Adding to the complexity is the lack of cyber literacy among citizens, even among the educated elite. Victims often fall prey not because they are naïve, but because they are unaware of their rights and the legal processes. The criminals exploit this ignorance, using scripted dialogues, legal jargon, fake identity cards, and digital courtrooms to construct a false reality. A person who has never interacted with the police or courts before is far more likely to believe that a video call from a "CBI officer" is real. This exploitation of legal fear and social shame is perhaps the most insidious weapon in the scammer's arsenal.

To tackle digital arrest, what India needs is a holistic, multi-pronged strategy—one that goes beyond just tightening the laws. First, there must be a formal statutory recognition of digital arrest as a distinct category of cybercrime, with comprehensive provisions addressing impersonation, psychological coercion, misuse of state emblems, and AI manipulation. Second, we need specialized cyber law enforcement units equipped with cutting-edge forensic

capabilities and jurisdictional agility. Third, the legal ecosystem must embrace technology-neutral principles that can adapt to emerging threats rather than constantly playing catch-up with innovation.Fourth, the judicial system must evolve its evidentiary standards to accommodate digital proof, AI simulations, and deepfake analysis, while ensuring the accused's rights are not compromised. Fifth, a robust victim support framework is urgently needed, including free legal aid, mental health counselling, and compensatory relief for those who have suffered emotional and financial harm. Finally, India must launch a massive digital literacy and public awareness campaign—spanning social media, educational institutions, and community platforms—to immunize the public against the psychological manipulation tactics of such scams.

In conclusion, digital arrest is not just a technological crime—it is a crisis of law, trust, and human dignity. It tests the responsiveness of our laws, the empathy of our institutions, and the resilience of our citizens. If left unaddressed, it threatens to create a climate of paranoia where every email, every phone call, and every message from an unknown number becomes a potential tool of fear. India stands at a legal and moral crossroads: it can either allow this silent pandemic of psychological cybercrime to spread, or it can rise to the occasion with a bold, empathetic, and future-ready legal framework. The time for cosmetic solutions is over; what we need is a systemic transformation—one that treats cybercrime not merely as a digital inconvenience but as a real, present, and escalating threat to the nation's legal sovereignty and the safety of its citizens.

References:-

Statutes & Legal Instruments

1. The Information Technology Act, 2000 (Act 21 of 2000).
2. Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
3. Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).
4. Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
5. Indian Penal Code, 1860 (now repealed, relevant for historical comparison).
6. Code of Criminal Procedure, 1973 (relevant for legacy procedural framework).

Books

7. Duggal, Pavan. Cyberlaw: The Indian Perspective, 6th edn, Universal Law Publishing, New

Delhi, 2023.

8. Sharma, Vakul. Information Technology: Law and Practice, Universal Law Publishing, New Delhi, 2022.

9. Singh, Ranbir. Cyber Crime and Law: A Study of Emerging

Journal Articles

10. Aggarwal, Kritika, "Understanding the Concept of Digital Arrest: A Legal Vacuum in Cybercrime Jurisprudence," (2023) 65(3) Journal of the Indian Law Institute 347.

11. Menon, N.R. Madhava, "Cyber Policing and Legal Dilemmas in India," (2022) 58(1) Indian Bar Review 12.

12. Banerjee, A. and Dutta, P., "Psychological Impact of Cybercrime Victimization in India: A Legal Perspective," (2023)

Government & Official Reports

13. Ministry of Home Affairs, Annual Report 2022-23, Government of India, available at https://www.mha.gov.in/sites/default/files/MHAAnnualReport2022-23.pdf (last accessed 19 Jul. 2025).

14. Indian Cybercrime Coordination Centre (I4C), Operational Framework Document, Government of India, 2021.

15. National Crime Records Bureau (NCRB), Crime in India Report 2022, available at https://ncrb.gov.in/en/crime-india (last accessed 20 Jul. 2025).

Web Sources & Media Reports

16. Press Trust of India, "Digital Arrests Are the New Cyber Threat: Delhi Police," The Hindu, (25 Feb. 2024), available at https://www.thehindu.com/news/cities/delhi/digital-arrest-scam/article67822193.ece (last accessed 19 Jul. 2025).

17. Sriram, Jayant, "What Is a 'Digital Arrest' and Why Is It on the Rise?", The Indian Express, (5 Mar. 2024), available at https://indianexpress.com/article/explained/digital-arrest-india-cybercrime-9219223/ (last accessed 20 Jul. 2025).

18. PIB, "Cybercrime Awareness Month: MHA Steps Up Citizen Cyber Safety," (Oct. 2023), available at https://pib.gov.in/PressReleasePage.aspx?PRID=1965027 (last accessed 18 Jul. 2025).