

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi-Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

EDITORIALTEAM

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 & Utkrish 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

Mrs.S.Kalpna

Assistant professor of Law

Mrs.S.Kalpna, 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.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS 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.

AN ANALYSIS OF DIGITAL ARREST: ITS LEGAL ASPECTS

AUTHORED BY - ASHWINI DOSHI

Abstract:-

In the era of digital transformation, the concept of application of the law has evolved beyond physical domain in the virtual kingdom. Digital unemployment, a relatively new concept, refers to the use of technology to restrict a person's access or digital movement, often as part of legal or administrative action. This document aims to explore the legal dimensions of digital unemployment, its legality of procedure, constitutional implications and the challenges it raises for privacy and due process. When analyzing the legal provisions, historical cases and the global context, the document tries to understand if the existing legal frameworks are adequate to accommodate said measure or if new legal paradigms are required.

Keywords: Digital Arrest, Right to Privacy, Cyber Crime, Information Technology, Bhartiya Nayay Sahita, Bhartiya Nagrik Suraksha Sahita.

Research Design:-

❖ Research Problem:-

Increase in the digitalization, the law enforcement agencies have begun to use technology not only to investigate but also to restrict individual rights in the digital arrest. The concept of digital detention, the reduction of digital freedoms, such as internet access, social networks, digital payments and online communication, grow important questions about legality, constitutionality and human rights. The absence of a legal framework makes this a gray zone not regulated in Indian law.

❖ Review of Literature:-

1. Digital Arrests: Understanding Their Legal Framework, Technology, and Case Studies in India

In this article, author wrote about digital arrest and its implementation in India through various effective laws.

2. *Joyti Chauhan, Digital Arrest: An Emerging Cybercrime in India, Volume 7, Issue 6 of International Journal of Law Management & Humanities on 2024.*

In this article, author wrote about the statistical data of digital arrest happening in India.

3. *D. Sarala, Analysis of a Digital Arrest Scam- Impersonation of Law Enforcement Officials, Volume 12, Issue 11 of International Journal of All Research Education & Scientific Methods on November 24.*

In this article, author wrote about digital arrest and its legality and constitutionality in India.

4. *Digital Arrest: A Legal And Technological Puzzle, on January 13, 2025.*

In this article, author wrote about digital arrest and explain its happening through various case laws.

❖ **Research Questions:-**

1. *What is the legal basis for digital arrest in Indian law?*
2. *Does digital arrest violate the right to privacy and liberty under the Constitution?*

❖ **Objectives of the Study:-**

1. *To define and conceptualize the term **digital arrest**.*
2. *To examine existing legal provisions in Indian law that could relate to or enable digital arrest.*
3. *To analyze constitutional implications including rights to privacy, free speech, and due process.*
4. *To evaluate judicial responses and case laws on digital restrictions.*
5. *To conduct a comparative analysis of how other countries regulate digital restrictions.*
6. *To propose recommendations for legal reforms or policy framework governing digital arrest.*

❖ **Research Methodology:-**

The research methodology to be undertaken in this research work shall be doctrinal using of primary and secondary data sources. The researcher will use e-legal resources as a doctrinal research for the research.

❖ **Hypothesis:-**

Digital arrest as a concept lacks a clear legal recognition and can conflict with constitutional guarantees unless they are properly regulated.

❖ **Scope of Research:-**

1. *Indian constitutional and legal framework*
2. *Legal interpretation of relevant laws (for example, IT law, BNS, BNS)*
3. *Emblematic judgments of the Indian courts*
4. *Policy documents and expert reports on digital rights and cyber security*

Introduction

In the increasingly digital world, the concept of digital arrests has been attracted to the spread of computer criminals and the need for modern mechanisms of law enforcement that could deal with online perpetrators. Digital arrests include detention of individuals for crimes committed in the digital empire, from hacking and financial fraud to online harassment, identity theft and even terrorism. Unlike traditional arrests, which include physical detention, digital arrests often focus on limiting human access to digital assets, monitoring online behavior and seizing electronic devices.

In India, where the Internet and digital services have risen sharply in recent years, there has been a parallel increase in digital crimes. The Indian government and coercive bodies adapt to this new landscape by developing laws and procedures that allow effective digital arrests and prosecution.

India has witnessed that the use of the Internet and digital services suddenly occurred, leading to hikes in digital crimes. *Recently Prime Minister Narendra Modi* addressed the nation in his "Mann Ki Baat" and raised concerns against fraud "digital arrest". Played audio-video A clip that showed a man in a police uniform and asked the victim to share his Aadhaar number to save her mobile number from blocking. Unlike traditional arrests, digital arrests usually limit the person in accessing his digital assets and freezing his physical movement by video. Digital arrests is the name of the technique of computer crime where fraudsters send messages or call calls or video calls to manipulate the publication of coercive officials or investigate agencies and capture fraud involving threats immediate digital restrictions.

Here, cyber criminals claim that an individual or their family members have been found in crime such as drug trafficking, money laundering or their card Aadhaar, SIM card or bank account were associated with illegal activities Therefore, they are arrested for video calls and sometimes pretend to be an online court for such a crime in court. It then forces the victim to

remain limited to the premises and bring them to keep the camera of their laptop or mobile phone. All this happens to create panic in them, to demand money through online transfers to ensure their release.

➤ What is a digital Arrest?

A digital arrest refers to the legal process of detaining an individual suspected of committing a crime in digital space. These arrests can involve physical detention, but more often, they imply restrictions on access to electronic devices, digital platforms and networks. The approach focuses on preventing continuous criminal activities online, confiscating electronic evidence and protecting the public from more damage.

Common types of crimes that lead to digital strikes include:

- i. *Cyber stalking and online harassment:* the use of digital platforms to harass, stalk or threaten people.
- ii. *Hacking:* unauthorized access to computer systems or networks.
- iii. *Phishing:* Fraudulent attempts to acquire confidential information such as passwords or financial details disguising themselves as a reliable entity.
- iv. *Cyber terrorism:* The use of Internet -based attacks to damage or interrupt critical systems, spreading fear or propaganda.
- v. *Financial Fraud:* Crimes such as theft of credit cards, identity theft or Ponzi schemes carried out online.
- vi. *Child and pornography:* the distribution or creation of illegal content that involves minors.
- vii. *False news and hate speeches:* the dissemination of false information or incendiary content that encourages violence or social disturbances.

The scammers are taking advantage of ignorance, fear, anxieties or blind trust of their goal and with the type of mental trauma, the victim loses his ability to think and act. In a recent incident with the president and managing director of a leading textile group in India, he was disappointed by a group that passed by officials from several government agencies and also led him to a virtual court, where the president of the impersonalized India of India was listening to the case.

In view of the incidents, *the Coordination Center of the Cyber Crime of India (I4C), affiliated*

with the Ministry of Interior, launched an advice, which says "not to panic, remain alert, CBI/ Police/ Custom/ ED/ Judges do not arrest it in a video call." Several messaging agencies have also issued guidelines to stay away from scammers.

Modus Operandi of Digital arrest: Here's How It Typically Works¹:

1. Initial Contact:-
 - a. *Medium:* Scammers usually initiate contact through phone calls, emails, or text messages. They may even use social media or messaging apps to reach their targets.
 - b. *Caller ID Spoofing:* Scammers often use caller ID spoofing technology to display a government or law enforcement agency's name or number, making it appear legitimate.
2. Impersonation and Authority Claim:-
 - a. *Posing as Officials:* The scammer pretends to be from a law enforcement agency, such as the FBI, IRS, or local police, or from a government agency like Social Security or the DMV.
 - b. *Official-Sounding Titles:* They introduce themselves with authoritative titles, such as "Officer," "Agent," or "Investigator," and sometimes give badge or ID numbers to seem authentic.
3. Creating a Sense of Urgency and Fear:-
 - a. *Fake Charges or Legal Trouble:* The scammer informs the victim that they are involved in serious legal trouble, such as tax fraud, identity theft, or an outstanding warrant. This "criminal charge" is often fabricated.
 - b. *Threat of Immediate Arrest or Legal Action:* Victims are told they face imminent arrest, deportation, or asset seizure unless they comply immediately. The scammer uses aggressive language, threatening to escalate the situation if the victim doesn't respond right away.
4. Demands for Payment or Information:-
 - a. *Payment Methods:* Victims are typically asked to make payment via non-traceable means like prepaid gift cards, cryptocurrency, wire transfers, or mobile payment apps.

¹ D. Sarala, Analysis of Digital Arrest Scam- Impersonation of Law Enforcement Officials, https://www.ijaresm.com/uploaded_files/document_file/D._Sarala_joIU.pdf, last visit at 11:44 am on 15/04/2025.

- b. *Personal Information*: Sometimes, instead of (or in addition to) asking for payment, the scammer will demand sensitive information such as Social Security numbers, bank account details, or credit card information for “verification.”
5. Follow-Up or Escalation Tactics:-
 - a. *Fake Documentation*: Scammers may send fabricated documents, such as “court orders” or “arrest warrants,” to make the threat feel more real.
 - b. *Repeated Calls or Messages*: To maintain the pressure, scammers may call multiple times or send several emails and texts, reinforcing the urgency and attempting to wear down the victim’s resistance.
 - c. *Third-Party Verification*: In some advanced scams, they may have a “supervisor” or “higher authority” get on the line to add legitimacy.
6. Extracting Payment or Information:-
 - a. *Instructions for Payment*: Victims are guided through the payment process, often told to stay on the line and not to speak to anyone else about the situation.
 - b. *Immediate Collection*: Once payment or information is provided, scammers may either disappear or continue to make demands, claiming additional fines or further penalties if the victim resists.
7. Exploiting Additional Opportunities:-
 - a. *Re-victimization*: Scammers may contact the victim again, claiming there are more fines, additional charges, or “settlements” required. In some cases, they even impersonate other “officials” to re-engage the same victim for more money.
 - b. *Selling Information*: If sensitive data is obtained, it may be sold on the black market or used in other fraudulent activities.

Key Takeaways:-

- a. *Law Enforcement Won’t Demand Payment*: Legitimate law enforcement and government agencies do not call people to demand payment or threaten immediate arrest over the phone.
- b. *Be Skeptical of High-Pressure Tactics*: Legitimate institutions provide time and options for verification, unlike scammers who press for immediate action.
- c. *Contact Official Channels*: Always confirm any such claims by reaching out directly to the alleged agency through known contact numbers or websites. Digital

arrest scams are highly manipulative and prey on people's fear of legal consequences, making it important to remain cautious and informed.

Legal Aspects of Digital Arrest under Indian Laws & International Conventions

❖ Legality of digital arrests in India:

There is no legal provision for the application of the law to make "arrests" through video calls or online monitoring. If you receive such calls, it is a clear scam. In fact, recently promulgated the new criminal laws do not provide any provision for the law agencies that make a digital arrest. Establishes that the citation is served electronically under *section 63 of the BNSS*. This section defines the form of the citation.

Section 532 of the BNSS, the judgment and the procedures can be maintained in electronic mode, through the use of electronic communication or through the use of electronic audio-video media.

❖ Tackling Digital Arrest:

If you are a victim of the digital unemployment fraud, the first step is to immediately inform your bank account and freeze your bank account. Present a complaint before the National Report Portal of Cybercrime (Cybercrime.gov.in). Always keep any evidence you have: call details, transaction details, messages, etc.

❖ Legal Framework for Digital Arrests under various laws in India:-

In India, the legal system has gradually adapted to deal with digital crimes. The primary laws and frameworks governing digital arrests include:

1. **Information Technology Act (2000):** The IT Act is the cornerstone of India's cyber law framework. It covers a wide range of cybercrimes such as hacking, identity theft, and the distribution of offensive content online. The IT Act empowers law enforcement agencies to investigate, arrest, and prosecute individuals for offenses committed in cyberspace.
 - i. **Section 66:** Deals with computer-related offenses, such as unauthorized access or data theft.
 - ii. **Section 67:** Covers offenses related to obscene content.

- iii. **Section 69:** Grants the government the power to intercept, monitor, or decrypt information in cases involving national security or cyber terrorism.
2. **Bhartiya Nayay Sahita (BNS):** Several provisions of the BNS apply to digital crimes. For example, Section 78 (stalking) and Section 351 (criminal intimidation by anonymous communication) are increasingly invoked in cases involving online harassment or cyber stalking.
3. **Bhartiya Nagarik Suraksha Sahita (BNSS):** The BNSS provides guidelines for arrests, searches, and seizures, which also apply to cases involving digital evidence. Law enforcement can confiscate electronic devices, freeze bank accounts, or block access to social media accounts as part of an investigation.
4. **The Personal Data Protection Bill (Pending):** This proposed bill will strengthen privacy protections and define how personal data can be collected, used, and processed in India. It will also establish penalties for data breaches and unauthorized access to personal information.

❖ *Technology Behind Digital Arrests:-*

Digital arrests often involve sophisticated technology and forensic techniques:

1. **Digital Forensics:** Law enforcement agencies rely on digital forensics to collect, analyze, and preserve electronic evidence. This can include recovering deleted files, tracking IP addresses, and decrypting communication on encrypted platforms.
2. **Online Surveillance:** Technologies like geo-fencing, IP tracking, and real-time monitoring of internet activity help authorities keep tabs on suspected criminals.
3. **Social Media Monitoring:** Platforms like Facebook, Instagram, and Twitter have become hotspots for illegal activities, from hate speech to financial fraud. Law enforcement agencies use artificial intelligence and machine learning tools to monitor suspicious activity on social media in real time.
4. **Data Interception:** Under certain provisions of the IT Act and national security laws, authorities can intercept communication on mobile networks, emails, or social media platforms. This technology is particularly useful in cases of cyberterrorism or organized crime.
5. **Blockchain Tracking:** As cryptocurrencies gain popularity, blockchain technology has become integral to digital arrests. Law enforcement agencies use blockchain analytics tools to track and trace illicit cryptocurrency transactions and bring criminals to justice.

❖ 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.

Analysis of the topic through case laws

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 schemes². 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 mode³.

➤ Case Laws:-

1. **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 call⁴.

2. 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.

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-energyemployee-duped-of-rs-71-lakh-124100700305_1.html

³ Ibd.

⁴ Joyti Chauhan, Digital arrest: An Emerging Cyber crime in India, <https://ijlmh.com/wp-content/uploads/Digital-Arrest-An-Emerging-Cybercrime-in-India.pdf>, last visit at 01:25 pm on 15/04/2025

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.

➤ Conclusion:-

The increase in digital unemployment is a notable threat to the cyber security of any nation. Scammers take advantage of the lack of awareness and weakness of people, either in personality or coercive measures. They use tricks about victims that they are in danger of suffering repercussions and, therefore, take away large amounts of money. They often use fear as a powerful tool to manipulate people and exploit their vulnerabilities to commit this crime.

To combat this growing crime, people must be proactive and conscious. Recently due to diffusion awareness, there are many bold examples of people who do not fall in the control of these criminals and establish an example for society. An authentication of two factors and a frequent change in the password can reduce the risk of unauthorized access to the accounts. One must be aware of phishing and protect their devices with reliable antivirus to improve privacy.

To protect one from digital unemployment, citizens should know about this cybernetic threat in constant change with collective knowledge and educated practices, and the

legislature must promulgate strong cyber security laws. Since it is also a cross -border crime union, in most cases the scammers call through SIM cards registered outside India. It is known that the *Indian code is +91*, so people should generally avoid collecting such calls to avoid falling into control of this crime.

Bibliography

Articles:-

1. *Analysis of Digital Arrest Scam: Impersonation of law Enforcement officials.*
2. *Digital Arrest: A legal and technological puzzle.*
3. *Digital Arrest: An emerging cyber crime in India.*
4. *Digital Arrest: Understanding their legal framework, technology, and case studies in India.*
5. *No one can arrest you through video calls: Digital arrest fraud on the rise.*

Website:-

1. <https://www.indiancybersquad.org/post/digital-arrests-understanding-their-legal-framework-technology-and-case-studies-in-india>
2. <https://ijlmh.com/wp-content/uploads/Digital-Arrest-An-Emerging-Cybercrime-in-India.pdf>
3. https://www.ijaresm.com/uploaded_files/document_file/D._Sarala_jolU.pdf
4. <https://restthecase.com/knowledge-bank/digital-arrest>
5. https://www.business-standard.com/finance/personal-finance/digital-arrest-fraud-explained-atomic-energyemployee-duped-of-rs-71-lakh-124100700305_1.html

Legislative Statutes:-

1. **Bhartiya Navay Sahita, 2023**
2. **Bhartiya Nagrik Suraksha Sanhita, 2023**
3. **Information Technology, 2000**
4. **Other Statutes.**