# ANALYSING DIGITAL ARREST THROUGH LEGAL PROVISIONS AND CYBERCRIMES: INSIGHTS FROM RECENT CASE STUDIES

Rakshita Adchitre, Symbiosis Law School, Pune

**ABSTRACT**

In today's age, with numerous types of cyber-crimes happening online, digital arrest is the most recent form of cyber-attack, which has caused hardships to many common people. Digital arrest has no legal basis in India or any other law across the world. Although, it sounds as legal as an actual physical arrest and even the cyber-criminals try their to pose as real officials but it is not valid at all. With such attacks having drastic consequences, it is critical to recognize and regulate the rights and duties vested in the victims of digital arrest. However, with the lack of any special law for such a new way of cyber fraud, recourse has to be sought to the existing legal framework, majorly within the information technology laws of India, i.e. the Information Technology Act, 2000, and The Information Technology Rules, 2011, and the subsequent jurisprudence. This article aims to venture into this exercise of placing digital arrest within the Information Technology Act, of 2000, and its subsequent precedents, along with precedents from different jurisdictions. This article adopts three methods of viewing this issue, firstly, it introduces the meaning of a digital arrest in the current context, then it analyses digital arrest in the backdrop of contemporary digital legal framework of India as well as the world. Secondly, it does a blanket analysis of digital arrest in the light of other prevalent cybercrimes happening all over the world. Thirdly, Case studies have been included to illustrate the cunning nature and manipulative strategies of the cybercriminals they deploy, to rob people. Lastly, it has been concluded with a summarised form of the article along with certain suggestive solutions for the common people (victims) and the government.

**Keywords:** Digital Arrest, Cybercrime, Information Technology Act, 2000,

## I. Introduction

We live in a digital age; everything we do is on the internet, which opens up a whole new world of opportunities as well as vulnerabilities.[1] The internet is a double-edged sword, it empowers us, but it also endangers us.[2] Cybercrime is any crime that involves computers as a means to deceive or defraud others.[3] The first-ever cybercrime incident occurred in 1834 in France,[4] and it has evolved into modern-day hacking, phishing, etc. Cybercrimes in India are evolving at an alarming pace, with digital arrest scams becoming a major concern. These scams are so sophisticated that even well-educated individuals fall prey to them.[5] It's disheartening to see daily newspapers filled with reports of these 'digital arrests'.[6]

"Digital arrest" is not a common legal or technical phrase. In legal situations, "arrest" refers to physical confinement by law enforcement. However, digital arrests were associated with cybercrimes like hacking, identity theft, and online fraud. Arrests increasingly require identifying and apprehending people who commit crimes through digital methods.[7]

This article tries to cover the severity of this critical issue by posing a question about the relevancy and adequacy of current legal digital laws. Part II studies the current digital laws governing technology in India and highlights the grey areas thereof. It will also cover, how digital laws are creating an impact in the real world, with a comparative study of the digital laws around the world. Part III studies the recent cases and their impacts, and finally Part IV attempts to answer the question of how we can overcome the issue and the possible solutions, along with the summary of observations made in this article.

### ii. Meaning of Digital Arrest

[1] Jess Conway, 'Living in a Digital World: the Good and the Bad' (*Medium*, 4 January 2021) <https://medium.com/digital-society/living-in-a-digital-world-the-good-and-the-bad-6e9bfe834be7> accessed 2 December 2024.

[2] Torila Quinker, 'The Internet: A Double-Edged Sword' *The Morung Express* (Nagaland, 3 December 2024) <https://www.morungexpress.com/the-internet-a-double-edged-sword> accessed 5 December 2024.

[3] Kate Brush; Michael Cobb, 'What is cybercrime and how can you prevent it?' (*TechTarget and Informa,* 3 September 2024) <https://www.techtarget.com/searchsecurity/definition/cybercrime> accessed on 22 December 2024.

[4] Arctic wolf, 'A Brief History of Cybercrime' (19 April 2024) <https://arcticwolf.com/resources/blog/decade-of-cybercrime/> accessed 20 December 2024.

[5] NDTV News Desk, 'Digital Arrest: People Are Losing Crores To Scammers. How To Remain Safe' (*NDTV,* 30 November 2024) <https://www.ndtv.com/india-news/digital-arrest-people-are-losing-crores-to-scammers-how-to-remain-safe-7138816> accessed on 7 December 2024.

[6] D. Sarala, 'Analysis of a Digital Arrest Scam – Impersonation of Law Enforcement Officials' (2024) XII(XI) International Journal of All Research Education and Scientific Methods (IJARESM) 2631,2636.

[7] Asmita Mallick and Adv. Prithwish Ganguli, 'Understanding of Digital Arrest: Definition, Methods and Implications' (*SSRN,* 27 September 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5019885> accessed 29 December 2024.

Semantically, Digital arrest should mean, detaining a person or keeping him under surveillance through the internet or any online communication channel or it may mean blocking access to electronic devices for an individual suspected of committing a crime in the digital space.[8] But, before the government of our country or other countries could bring such a provision for conducting digital arrests, given the ever-fast-paced digitalization of almost all government processes ranging from the filing of forms to the official summons of the Court,[9] the criminals of cyberspace proved to be much more ahead.

They inculcated this new way to fraud people of their hard-earned money, by putting them under a digital arrest. Cyber law expert and advocate Pawan Duggal explained, "Digital arrest is the phenomenon of trying to put somebody in a sense of fear and panic and thereafter going ahead and extorting money from the said person under some mistaken notion so as to make the said person a victim of a cybercrime.[10]"

These scammers threaten people on video calls, inducing them to transfer huge sums of money to their bank accounts. They use illegal bank accounts to transfer illegal money, studio-modelled police stations, fake ID cards, and fake uniforms to defraud people.[11] They usually create a stressful environment during the video call to end up making the victim anxious. These "arrests" have been taking place by masterminds sitting abroad. Scammers working under these masterminds make use of the innocence of people, making them believe that they are under cyber or digital arrest, highlighting the psychological relevance of the subject too.[12]

Digital arrest perpetrators commit fraud, extortion, and impersonation. Extortion is a criminal offense, and those implicated may face jail and fines. Victims are frequently forced into moving money to specific accounts. If the scammers succeed, they may engage in money laundering, which is prohibited. Conspirators in these scams could face accusations of conspiracy to commit fraud or other felonies. Victims who suffer financial losses may file legal actions against the culprits, potentially resulting in compensation awards. Because criminal scams can cross countries, international law enforcement cooperation is critical in locating and prosecuting perpetrators.

---

[8] Indian Cyber Squad, 'Digital Arrests: Understanding Their Legal Framework, Technology, and Case Studies in India' (4 October 2024) <https://www.indiancybersquad.org/post/digital-arrests-understanding-their-legal-framework-technology-and-case-studies-in-india> accessed on 16 December 2024.

[9] Bhartiya Nyay Suraksha Sanhita, 2024 (BNSS), s.64.

[10] NDTV News Desk, n3.

[11] Brielle Burns, 'Do Not Panic: India's Prime Minister Warns Against Digital Arrest Scams' (*News.com.au,* 28 October 2024)<https://www.news.com.au/world/asia/do-not-panic-indias-prime-minister-warns-against-digital-arrest-scams/news-story/33aca1e1f2956b6d7a799cff0f82929f> accessed 20 December 2024.

[12] Dia Rekhi, 'You Are Under Digital Arrest: How Fake Cop Scams Are Draining Victim's Bank's Accounts' *Economic Times* (India, 4 November 2024)<https://economictimes.indiatimes.com/tech/technology/you-are-under-digital-arrest-how-fake-cop-scams-draining-victims-bank-accounts/articleshow/114885522.cms?from=mdr>accessed 21 December 2024.

### iii. Major Digital Laws in India

The Internet was introduced to India in the year 1995; since then, the flow of the network has always been expanding in this country. With the advent of the internet and technology and an increase in cybercrimes, data privacy has become a new concept. Disadvantages of the internet were on the surge, and the nation's security was on hold. Thus, the legislature passed laws in order to preserve users' data and to decrease cybercrimes. With the rising cases of Digital arrests, organizations such as Enforcement Directorate and Indian Cybercrime Coordination Centre (I4C) are playing a major role by releasing an advisory for the citizens of India.[13]

#### *A. The Information Technology Act, 2000*

One of the oldest of such laws was The Information Technology Act, of 2000 ("**Act**") which focused on covering many intricacies of the Internet. Containing 94 sections with one major amendment—the **IT (Amendment) Act, 2008,**[14] the law covers significant areas of digital complexities, including cybercrimes such as phishing, identity theft, publishing sexual material online, hacking, cyber obscenity, cyber terrorism, cheating using a computer, etc[15] (section 43[16]).

#### a) *Section 69, 75*

Section 69 of the IT Act[17] provides the government with the power to block any information reaching the public from online platforms through intermediaries or authorized government agencies if the information, in context, is against the nation's sovereignty, integrity, defence, and peace. This act has been advocated against since many years for the reason of being unconstitutional and government authorities being using it arbitrarily. Although this section has helped authorities to fight against rising digital arrest scams, as it helps them to identify, track, monitor and block the activities of perpetrators.[18]

Since perpetrators operate from sitting outside the territorial boundary of India in the hope of escaping liability, Section 75 helps authorities to catch them irrespective of the fact that they are not within the territorial boundary of India. This section has been proven of great help to the authorities as it involves offenses involving computer systems.[19]

---

[13] Vajiram & Ravi, 'Digital Arrest Scams: ED Charge Sheet & I4C Advisory to Protect Citizens' (Vajiram & Ravi, 2023) https://vajiramandravi.com/upsc-daily-current-affairs/mains-articles/digital-arrest-scams:-ed-charge-sheet-i4c-advisory-to-protect-citizens/ accessed 13 December 2024.
[14] Information Technology (Amendment) Act 2008 (India).
[15] Mayashree Acharya, 'IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties' (*cleartax,* 17 April 2024)< https://cleartax.in/s/it-act-2000> accessed on 9 December 2024
[16] Information Technology Act 2000 (India), s 43.
[17]Information Technology Act 2000 (India), s 69.
[18] Indian Cyber Squad, n7.
[19] Information Technology Act 2000 (India), s 75.

**b) *Section 66, 66A, 66B***

These sections deal with cybercrimes. According to section 66, if an individual engages in any offences listed in section 43 of the IT Act, he or she shall be subjected to the punishment.[20] Section 66A penalizes sending offensive messages online[21], whereas section 66B penalizes knowingly receiving any stolen computer resources or devices.[22] In the famous *Shreya Singhal v UOI* case, the SC has struck down Section 66A as it was held as being unconstitutional against the constitutional provisions.[23] It was held that it infringes upon the fundamental right of freedom of speech and expression[24] (Article 19(1)(a) of the constitution).

**c) *Information Technology Rules, 2011***

In 2011, the Central Government released various rules for the proper implementation of the Act: the Information Technology ("**IT**") (Intermediaries Guidelines) Rules, 2011; IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; IT (Guidelines for Cyber Cafe) Rules, 2011; IT (Electronic Service Delivery) Rules, 2011. All these rules were brought up in order to further the objective of the Act as mentioned in its Preamble and safeguard people against the activities of cybercriminals. But as technology is evolving now at a very fast pace, the cunning cyber-attackers have brought in newer ways to fraud and rob people, Digital arrest being one of them. Therefore, even after having quite sound laws and rules on the regulation of information technology, we need stronger implementations and more coherent laws to prevent such losses to the Common Man of India.

***B. Digital Personal Data Protection Act, 2023***

Shri Krishna committee's report[25] on the topic of the introduction of data privacy role in India in the year 2018, suggested many reforms in the IT Act, of 2000. The Indian Parliament in the year 2023 passed the Digital Personal Data Protection Act[26] to protect the data of individuals based on the report, providing the Act with certain powers.[27] This Act was passed to overcome flaws of the IT Act, of 2000. Under this Act, personal data of individuals can be used for lawful purposes having them the right to permanently erasure of data.

[20] Information Technology Act 2000 (India), s 66.
[21] Information Technology Act 2000 (India), s 66A.
[22] Information Technology Act 2000 (India), s 66B.
[23] *Shreya Singhal v Union of India* (2013) 12 SCC 73.
[24] Constitution of India, art (19)(1)(a).
[25] Justice Shrikrishna Committee, *Report of the Committee of Experts on a Data Protection Framework for India* (2018) Ministry of Electronics and Information Technology, Government of India.
[26] Digital Personal Data Protection Act 2023 (India).
[27] Anirudh Burman, 'Understanding India's New Digital Protection Law' (Carnegie Endowment for International Peace, 23 October 2023 <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en> accessed 28 December 2024.

Data Fiduciaries have a poignant role under this Act. They are differentiated into different categories such as SDFs (Significant Data Fiduciaries) based on the sensitivity of the data.[28] They are even provided with the power to obtain data without getting consent in certain cases. Certain sections of the law have been a point of debate, such as section 17(2)(a) of the law which provides the Government with the power to exempt this law from certain state agencies under sensitive circumstances.[29] The DPA board covered under this act is entrusted with the power to frame regulations and issue penalties.

### iv. Major Digital Laws in the World

#### *A. Budapest Convention on Cybercrime*

With the increasing number of cybercrimes around the globe, the first-ever initiative to redress this issue was brought up by the Council of Europe along with Canada, South Africa, Japan, and the USA in the year 2001, as the Budapest Convention on Cybercrime. India has refrained to sign the convention. To this date, 67 countries are part of this convention, whereas Russia and Ireland have backed off from signing to protect its national integrity. It focuses on bringing countries together against cybercrimes and hacking, formalizes national laws, and criminalizes certain actions done through computers.

#### *B. UN Cybercrime Treaty*

The UN too has come forward in negotiating a new international binding treaty to confront surging cybercrime cases globally in the form of the UN Cybercrime Treaty. Focusing on cross-border surveillance and cooperation, this treaty has been through many criticisms as well because it incorporated several non-computer-based crimes such as drug trafficking, firearms trafficking, etc. It provides nations with the power to apply laws extraterritorially. Passive Personality Jurisdiction, introduced by Article 22, permits signatory states to hold any of their nationals residing outside the boundary to prosecute, attracting criticism.[30] Some states are terrified of the terminology being used in the treaty as it incorporates white hat hackers and authentic cyber investigators.

#### *C. General Data Protection Regulation (GDPR), 2018*

General Data Protection Regulation (GDPR), 2018 governs the data of the people of European Union. It even applies to cross-border organizations if they are operating EU people's data.[31]General Data Protection Regulation (GDPR) came into force to protect the privacy of people. It is relevant to study General Data Protection Regulation in the context of Digital

[28] ibid.
[29]Digital Personal Data Protection Act 2023 (India), s (17)(2)(a).
[30]Draft UN Cybercrime Treaty 2023, art 22.
[31] GDPR.eu, 'What is GDPR? The EU's General Data Protection Regulation Explained' (GDPR.eu, 6 July 2020) <https://gdpr.eu/what-is-gdpr/> accessed 29 December 2024.

arrests because it is one of the strongest Digital Laws in the world. It has provided organizations with the guidelines to collect and process data with extreme legitimacy.[32] Several provisions of General Data Protection Regulation align with the new Digital Personal Data Protection Act, of 2023 such as the Right to be forgotten, the Right to rectification, etc. It includes regulations for the data controller if the data is being obtained other than the original owner such as the requirement of permission from the owner to transfer data and the need to describe the data.[33] There are provisions for stricter penalties if the data is breached and if the data is breached, it should be reported within 72 hours.[34]

## V. Case Studies

### *A. Elderly woman becomes the victim of the Digital Arrest Scam in Mumbai, losing ₹ 1.15 crores.*

#### *a) Case background*

As per the reports of Times of India, fraudsters impersonating themselves as members of the Special Investigation Team (SIT) of Delhi Special Police, scammed a 78-year-old woman. They threatened her that she was under investigation and due to stress she transferred 1.15 crores to their account. They threatened her by saying that they had found a courier with her name on it, which contained 2,000 mg of mephedrone and 2,000 US dollars. After realizing that she was scammed, she immediately called the Cybercrime Police Helpline 1930.

#### *b) Analysis*

In this case, the attacker impersonated himself as an official by using various props like fake uniforms, logos, flags etc. He created a panic situation for the old lady, to act immediately without giving her time to think about the consequences. Threatening her by using names of drugs such as mephedrone directs us to the point that they are well versed with the knowledge of drugs and are vigilant. This leads us to the most crucial aspect of such crimes, the tactics of cybercriminals i.e. how intricately, they play with the psychology of the common people and make people fall into their trap.

### *B. Ahmedabad: A gang of cyber thugs scammed a senior citizen, and lost ₹ 17 lakhs.*

#### *a) Case background*

[32] TechTarget, 'What is GDPR? (General Data Protection Regulation)' (TechTarget, 5 January 2025) <https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR> accessed 5 January 2025.
[33] ibid.
[34] Wired, 'What is GDPR? The Summary of the EU's Data Protection Legislation' (Wired, 24 May 2018) <https://www.wired.com/story/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018/> accessed 5 December 2024

As per the reports of ETV Bharat, cyberthugs impersonated themselves as inspectors of the Customs Department, called the elderly man and claimed that they had digitally arrested the old man because they had found 16 bogus passports, 58 ATM cards, and 140 GM MD drugs in his parcel. After receiving information about the same, Cyber Police started an investigation. A Cambodian gang was running the whole scam involving a Russian person, Anatoly Mironov. Anatoly Mironov was a gatekeeper who used to help the gang members to transfer money to China. After further investigation, it was found that these scammers used to transfer money into other accounts or crypto currencies.

***b) Analysis***

This case highlights how efficiently these fraudsters use terror tactics on victims, frequently appearing as law enforcement or government personnel, to coerce them into complying. These people use the victim's vulnerability and lack of awareness, highlighting significant repercussions. With the involvement of scammers from outside of India, the case underscores the cross-border nature of the scam, indicating how the Internet is a global space, which cannot be regulated without the collaboration and cooperation of nations across the world.

***C. Karkala: A 57-year-old man fell prey to the threat of "Digital Arrest", and lost ₹ 8.93 lakhs.***

***a) Case background***

57-year-old Shivanand V. Padmashali informed the Karkala Town Police that he received a call on December 13, 2024, from a person claiming to be an officer from the Mumbai Crime Branch. Scammers said that he was digitally arrested because of the transfer of 30 lakhs from his account to different accounts**.** They further said that to "verify" his bank account, he needed to transfer them money. Because of this, he ended up transferring money to the account of one Pavan Kumar Gujar. Police have registered the case under Section 308 (Extortion) of Bharatiya Nyay Sanhita and under Section 66 (D) of Information Technology Act.

***b) Analysis***

Scammers creating a tense environment and playing with the emotions of victims is one of their ways of defrauding and fetching out the money. Same as in this case, the scammer impersonated himself as an officer, gained the trust of the victim. Their aim is to deprive the person of their ability to think rationally and to make him so vulnerable that he ends up losing money.

These case studies are perfect illustrations of the audacity and ingenuity of cybercriminals who utilize fear and misleading information to deceive victims into believing they risk severe legal consequences and financial loss. People must adopt a proactive and vigilant approach to cybersecurity to tackle this growing cybercrime.

To reduce the likelihood of unauthorized access, cyber hygiene practices like two-factor authentication and regular password changes are crucial. Being cautious of phishing attempts, securing devices with trustworthy antivirus software, and utilizing Virtual Private Networks (VPNs) to enhance privacy are all crucial safety measures.