DIGITAL ARREST SCAMS AND THE CONSTITUTIONAL RIGHT TO PERSONAL LIBERTY UNDER ARTICLE 21 - A CRITICAL ANALYSIS

Roshani Pal, LL.M., Atal Bihari Vajpayee School of Legal Studies, Chhatrapati Shahu Ji Maharaj University, Kanpur[1]

Lalit Shukla, LL.M., Atal Bihari Vajpayee School of Legal Studies, Chhatrapati Shahu Ji Maharaj University, Kanpur[2]

ABSTRACT

The rapid expansion of digital communication technologies in India over the past decade has significantly enhanced connectivity, accessibility, and efficiency in everyday life. However, this digital transformation has simultaneously given rise to sophisticated forms of cyber-enabled crimes that exploit technological platforms and public vulnerability. Among the most alarming emerging threats is the phenomenon popularly referred to as "digital arrest" scams. In these scams, fraudsters impersonate officials from law enforcement and investigative agencies, such as CBI, ED, cybercrime units, and even judicial authorities. Through phone calls, video conferencing platforms, or messaging applications, they falsely inform victims that they are under investigation for serious criminal offences such as money laundering, drug trafficking, or financial fraud. The perpetrators then claim that the victim is under "digital arrest" or "virtual custody", instructing them to remain isolated, avoid contacting others, and comply with their directives. These fraudulent actors often use intimidation tactics, fabricated legal documents, and continuous surveillance through video calls to create an atmosphere of fear and urgency. Victims are threatened with immediate arrest, freezing bank accounts, seizure of assets, or public exposure unless they cooperate. Under such psychological pressure, victims are frequently coerced into transferring large sums of money under the guise of "verification," "security deposits," or "temporary investigation procedures". This research examines the phenomenon of digital arrest scams through the constitutional lens of Art. 21 of Indian Constitution. While the perpetrators of these scams are private actors, the coercive tactics they employ effectively simulate unlawful detention and intimidation, thereby infringing upon an individual's sense of personal liberty, autonomy, and dignity. This research

[1] Post-Graduate in Law (LL.M.), Atal Bihari Vajpayee School of Legal Studies, Chhatrapati Shahu Ji Maharaj University, Kanpur

[2] Graduate in Law (LL.B.) Chhatrapati Shahu Ji Maharaj University, Kanpur

argues that such forms of digital coercion create a quasi-custodial environment in which victims are psychologically restrained and deprived of their freedom of action, raising important constitutional questions about the protection of liberty in the digital age.

Keywords: Digitally Arrest Scams, Personal Liberty, Cyber Crimes, Cyber Constitutionalism; Substantive Due Process, Cyber Policing, Virtual Coercion.

INTRODUCTION

The digitally transformed India has integrated systems of communication, governance, commerce, and social interaction. Online environments have been adopted by the Government, banking, and even the judiciary. While the shift to digitization has improved access and efficiency, it has also facilitated new types of exploitation. Cyber fraud has evolved from attempts like phishing and OTP scams to more sophisticated frauds using the psychology of the victim. One such alarmingly sophisticated fraud is what is called the "digital arrest scam".[3]

In such scams, criminals impersonate officials from the Central Bureau of Investigation, or the Enforcement Directorate, or the Reserve Bank of India, or even various police departments. Victims of these scams are communicated via video calls or other messaging platforms and are told that they are involved in serious crimes like money laundering, illegal drug trafficking, or tax evasion. Victims are warned that there are court warrants against them, bank accounts will be frozen, or they will be arrested. To not be arrested, they have to stay connected to the video call, and in some cases, for hours, or even days. During this time, the victim is continuously monitored, and there is extreme transfer of money, which is called "verification" or "settlement" amounts, to the scammer.

In contrast to typical forms of fraud, digital arrest scams execute a form of impersonation of state power and criminal law's obtrusive mechanisms, creating a psychosocial state similar to illegal confinement, where although there is no actual imprisonment, victims undergo extreme emotional stress involving the loss of control and autonomy, the fear of actual imprisonment, & so-called obstruction compliance. This raises the question of whether such forms of technologically induced psychological manipulation constitute an infringement of India's

[3] Siri Vadlamudi, *Digital Arrest Scams in India: An Analysis of Socio-Demographic Vulnerability, Fear and Financial Loss*, in International Conference for Student Academic Research ICONSTARS 2025, (2025), https://doi.org/10.65694/icgst2025-cp01-003.

Constitution, Art. 21.[4]

Art. 21 of the Constitution of India states, *"No person shall be deprived of his life or personal liberty except according to procedure established by law."* For decades, judiciary has interpreted these words to include the right to one's dignity, the right to privacy, the right to autonomy, & right to no arbitrary action by the state. This paper presents the argument that digital arrest scams constitute a novel form of deprivation of liberty, and that the State's constitutional obligations breach the physical realm of confinement and require the State to protect the citizenry from digital forms of imprisonment.

THE DEVELOPMENT OF PERSONAL LIBERTY UNDER ARTICLE 21

The development of the interpretation of Art. 21 has been significant. The first interpretation of Art. 21 was in *A. K. Gopalan v. State of Madras*,[5] where court mentioned that "the procedure established by law" was any procedure that had been placed by a legislature that was competent, regardless of whether such a procedure was fair. This was a formalistic view, which kept legislative action free from fair scrutiny.

This view, however, was changed in *Maneka Gandhi v. Union of India*,[6] wherein court stated that the procedure in Art. 21 of the Indian Constitution must be "right, just and fair", and that it must not be arbitrary, capricious, or oppressive. This was the first time that substantive due process was invoked in Indian jurisprudence, and for the first time, Art. 14, 19, and 21 were referred to as the golden triangle of rights.

Thereafter, court further widened the scope of personal liberty to include a variety of rights. In *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*,[7] court ruled that the right to life includes the right to live with human dignity. In *Sunil Batra v. Delhi Administration*,[8] court held that prisoners, too, possess fundamental rights, which may be restricted only to the extent that is lawful.

[4] Diksha Diksha & Dr Neetu Singh, *Arrest Scams In The Digital Era: Legal Loopholes And Regulatory Challenges*, 6 Int'l J. Rsch. Publ'n & Revs. 476, (2025), https://doi.org/10.55248/gengpi.06.1125.3831.
[5] AIR 1950 SC 27.
[6] (1978) 1 SCC 248.
[7] (1981) 1 SCC 608.
[8] (1978) 4 SCC 494.

Most notably, court, in *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.*,[9] recognized the "fundamental right to privacy as part of the right to life and personal liberty enshrined in Art. 21". The verdict acknowledged the right to informational self-determination and protection against state surveillance as the core of liberty in the contemporary digital world.

These developments clarify that Art. 21 goes beyond the protection of physical incarceration. It encompasses the protection of psychological integrity, self-determination, and freedom from external control. Any infringement of liberty that involves a loss of self-control and psychological integrity must consider the digital arrest scams that mimic state coercion & psychological captivity of victims.

The phenomenon of digital arrest scams invites a deeper constitutional inquiry into whether deprivation of liberty must necessarily involve physical confinement or whether coercive digital environments can produce a similar constitutional injury. Traditional legal discourse historically associated deprivation of liberty with physical restraint or detention by state authorities. However, modern constitutional jurisprudence has gradually expanded this conception to include psychological coercion, informational manipulation, and other non-physical forms of domination that significantly impair individual autonomy.[10]

In several judicial pronouncements, court has emphasized that personal liberty under Art. 21 cannot be interpreted in a narrow or pedantic manner. Rather, the expression "personal liberty" has been interpreted broadly to include a cluster of rights that enable an individual to exercise autonomy and freedom of choice. When an individual is compelled, through fear and intimidation, to remain connected to a digital communication channel for prolonged periods and is psychologically conditioned to believe that disobedience will lead to arrest or legal consequences, the resulting situation functionally resembles detention.

The defining feature of detention is the absence of meaningful freedom to disengage. In digital arrest scams, victims often remain on video calls for hours or even days under constant supervision by fraudsters posing as law-enforcement officers. Victims are instructed not to communicate with anyone else, not to disconnect the call, and not to leave their location. The combination of surveillance, threats of criminal prosecution, and fabricated legal

[9] (2017) 10 SCC 1.
[10] *Supra* note 1.

documentation produces an environment where the victim believes that compliance is legally mandatory.

This environment can be conceptualized as a form of virtual detention, wherein the individual's liberty is constrained not through physical force but through technologically mediated psychological domination. The constitutional injury lies in the erosion of decisional autonomy. The victim is deprived of the ability to independently evaluate choices or seek external assistance due to the artificially constructed authority of the impersonator.

From a constitutional standpoint, such manipulation implicates not only personal liberty but also dignity and mental integrity. The jurisprudence under Art. 21 has repeatedly recognized that dignity forms the core of the right to life. When individuals are forced into humiliating situations where they are compelled to justify their innocence before fictitious authorities and surrender personal information or financial resources, the dignity of the individual is directly compromised.

Furthermore, the jurisprudence of wrongful confinement under criminal law demonstrates that physical barriers are not always necessary for confinement to occur. Courts have acknowledged that restraint may arise from threats or intimidation if such threats effectively prevent a person from exercising freedom of movement. By analogy, digital arrest scams operate through psychological barriers rather than physical ones. The victim is technically free to disconnect the call, yet the perceived consequences of doing so, arrest, seizure of property, or criminal charges, create a coercive environment that neutralizes this freedom.

In this sense, digital arrest scams represent a technologically mediated extension of unlawful restraint. The coercive authority exercised by fraudsters imitates the legal power of the State but operates entirely outside the framework of law. This imitation of sovereign power transforms a simple financial fraud into a constitutional concern. The misuse of state symbols, fabricated warrants, and impersonation of public authorities generates an illusion of lawful coercion, thereby exploiting citizens' trust in legal institutions.[11]

Consequently, recognizing digital arrest scams as a form of virtual deprivation of liberty allows constitutional law to respond more effectively to emerging technological threats. Such

[11] *Supra* note 2.

recognition does not imply that every cyber fraud constitutes a constitutional violation. Rather, it highlights that certain technologically facilitated crimes, particularly those involving sustained psychological coercion and simulated state authority, can produce harms comparable to unlawful detention. In this context, the protection of liberty under Art. 21 must evolve to encompass new forms of coercion that operate within digital environments.

FRAMING DIGITAL ARREST AS A DEPRIVATION OF LIBERTY

Digital arrest scams rely on the elements of intimidation, impersonation, and psychological manipulation. Victims are instructed to keep the phone on for as long as possible, to avoid any communication with their family, and to refrain from contacting a lawyer. Many scammers show falsified documents with government insignia, make video calls, and/or use backgrounds that mimic government offices. Everything is aimed at creating a captive atmosphere of fear and control.

From a constitutional viewpoint, this scenario, in functional terms, resembles unlawful detention. While there may not be actual physical detention, the affected individual is not autonomous. Coercive and dominant state power is exercised in order to ensure compliance. This leads to the question, Is it possible to be deprived of one's freedom without being physically restrained?

In Indian law, the right to liberty includes freedom from arbitrary constriction of one's movement & ability to make decisions. In *Joginder Kumar v. State of Uttar Pradesh*,[12] court stated that arrests should not be made as a routine process and that there needs to be a valid reason and explanation supporting an arrest. In *D.K. Basu v. State of West Bengal*,[13] court outlined various processes to ensure that custodial and arbitrary detention do not occur.

These cases show how the courts are sensitive to the misuse of state power when it comes to making physical arrests. Arrests that are being made digitally have no legal grounds. They are also threatening, isolating, and surveilling, which, psychologically, are very close to arrest. Because of this, the fact that the perpetrators of these acts are private actors does not diminish the gravity of the constitutional injury that these acts cause, which is the injury that Art. 21 attempts to protect. In addition, Puttaswamy's ruling delineated that right to privacy also

[12] (1994) 4 SCC 260.
[13] (1997) 1 SCC 416.

includes the right to be free from unconsented surveillance. Digital arrest scam perpetrators typically instruct their targets to turn on their cameras, share their screens, give bank details, and expose personal information. Such coercive surveillance is a violation of the victim's informational self-determination. Therefore, digital arrest scams must be understood as a new type of constitutionally illegitimate virtual exercise of the freedom to lose control over oneself, which warrants both a legal and a political response.[14]

STATUTORY FRAMEWORK - ARE EXISTING LAWS ADEQUATE?

The immediate regulation of digital arrest scams does only fall into the purview of constitutional law because of its prominent constitutional concerns. It also falls into the realms of statutory criminal law and cyber law. In India, this is regulated under IT Act, 2000 & BNS, 2023.

Section 66D of IT Act, 2000, which criminalizes cheating by personation, gains a particular interest since one of the main acts of digital arrest scams is impersonating officials. Additionally, Section 66C speaks of Identity Crimes, specifically, fraudulently using electronic signatures, passwords, and other means of unique identification. The BNS, 2023, mentions cheating, criminal intimidation, impersonation of a public servant, and extortion as relevant offences. There are provisions for cheating and dishonestly inducing delivery of property, criminal intimidation, and personation, which apply in the context where fraudsters threaten digital arrest scam victims with an arrest order. Where victims are legally compelled to transfer funds, extortion is clearly applicable.[15]

Even though the above-mentioned offences are available in statutory form, there are still significant challenges to enforcement. Digital arrest scams are carried out by cross-border syndicates that operate in a pseudonymous manner, using encryption, making enforcement particularly challenging. There are jurisdiction issues, complexities in evidence, and a time lapse in victim reporting that are all detrimental to the goals of criminal enforcement. Statutory remedies concern primarily monetary loss. However, the law is silent on the victims' psychological distress, mental imprisonment, fear, & prying of the law. These concerns

[14] Amrutha Karamvalappil, *The Revolution of Digital Scams and Right to Privacy in India*, 7 Int'l J. For Multidisciplinary Rsch., (2025), https://doi.org/10.36948/ijfmr.2025.v07i03.45161.
[15] *Id.*

highlight the importance of viewing these offences as frauds not only of an economic nature, but of the breach of the constitutional right to liberty and dignity.

THE STATES' RESPONSIBILITY AND POSITIVE OBLIGATION UNDER ARTICLE 21

This raises the concern of whether Art. 21 applies to digital arrest scams given that they are conducted by private individuals. This is instance with fundamental rights which have a vertical operation with respect to the State. However, with time, the courts have had to recognize the State's positive obligation when it comes to protecting individuals from the violation of their rights by other private individuals. In *Vishaka v. State of Rajasthan*,[16] court stated that the State is required to provide guidelines in the absence of adequate legislation to that effect & Court stated that an omission to do so is a violation of the Constitution.

The same goes for *Nilabati Behera v. State of Orissa*,[17] where the State was held liable for compensating for a custodial death & Court reiterated that the State had a positive obligation under Art. 21 to protect life and liberty. Considering this reasoning, the State's responsibilities include jurisdictionally appropriate cyber policing and creating digital arrest fraud awareness campaigns, alongside technological and judicial remedies. When the digital arrest frauds get entrenched, & State authorities do not act to mitigate them, the State may face constitutional claims. Of great importance is the doctrine of positive obligations in digital situations. While the State is in favour of digital governance, digital payment systems, and digital identification, it also needs to secure infrastructure for safe cyberspace. The protection of the 21st century is also protection in cyberspace.

PSYCHOLOGICAL CONSTRAINT AND BROADENING OF LIBERTY

The evolution of case law under Art. 21 has treated dignity as an intrinsic facet of life and liberty. In this context, *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*[18] is especially instructive. Court in *Common Cause v. Union of India*,[19] noted the importance of dignity of life as involving autonomy & preservation of control over one's decisions.

[16] (1997) 6 SCC 241.
[17] (1993) 2 SCC 746.
[18] (1981) 1 SCC 608.
[19] (2018) 5 SCC 1.

Digital arrest scams further violate the dignity of victims. The victims of such scams, which will often include members of vulnerable groups, experience humiliation, intimidation, and a significant loss of control over their situation. They may be victims of instructions to cut off all contact with family members who may be able to assist them. Severe cases of such protracted coercion may lead to the victim suffering trauma, anxiety and may even create a risk of suicide.

If Art. 21 does protect autonomy and decisional freedom, then psychological coercion, which ensures the absence of free choice, cannot simply be dismissed as a case of fraud. The loss is not only monetary but is also a loss of the defendant's autonomy which is surrendered under the compulsion of state-backed violence. The challenge is of a conceptual nature. The liberty of a person must encompass the absence of a person being subjected to digital and psychological control. Just as a person being subjected to custodial torture, and who is not convicted, is a violation of Art. 21, so is the case of a person being subjected to sustained digital coercion which resembles arrest.[20]

DIGITAL CONSTITUTIONALISM AND COMPARATIVE INSIGHTS

Constitutional frameworks across the globe are facing similar issues of technology induced rights violations. The European Court of Human Rights has, through the lens of unlawful digital intrusion, interpreted Art. 8 of the European Convention on Human Rights concerning the right to privacy and, therefore, the right to not be surveilled. This is also the case in the Indian jurisdiction in *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.*,[21] wherein court has, in effect, understood the essence of the need to revise the constitution to accommodate technology.

Constitutional digitalism entails the need for fundamental rights to adapt to technological advancement. The limitation of liberty to physical space, i.e. that a person is not free to leave a room, is a restriction that has become antique. In a world that is essentially digital in nature for most of the societal, economic and professional interactions, the absence of freedom to choose in the digital world is as restrictive as it is in the physical world. The digital arrest scam phenomenon also includes the exploitation of sovereign authority images, including police

[20] Vrajlal K. Sapovadia, *Unraveling Digital Arrest Scams in Gujarat: A Deep Dive into Fraud, Systems, and Society*, 2025 SSRN Elec. J., https://doi.org/10.2139/ssrn.5318969.
[21] 2017 SCC 1.

insignia, court logos, and state seals. The effect of state imagery being used in this manner is more pronounced. The State, therefore, has a strong justification for being concerned about the impersonation of a public authority, and for the need to improve the means for verifying the identity of people in electronic communications.

Unlike Australia, the US and some other jurisdictions have, to varying degrees, recognized certain types of coercive fraud as posing due process concerns. The precise details of constitutional frameworks may differ, but there is a common denominator. When the means of a particular legal process are abused in a way that subverts the legal control and protection of an individual, the law must respond. While the recognition of digital arrest scams as a threat to personal liberty is normatively compelling, the institutional mechanisms required to address such threats remain underdeveloped. The legal system must confront the structural difficulties associated with regulating technologically sophisticated fraud that operates across jurisdictional boundaries and relies on rapidly evolving communication platforms.

One of the principal challenges lies in the fragmentation of regulatory responsibility. Cybercrime investigations in India involve multiple institutional actors, including local police authorities, specialized cybercrime units, telecommunications regulators, financial institutions, and central investigative agencies. This multiplicity of actors often results in procedural delays and jurisdictional ambiguity. Victims may find it difficult to determine which authority should receive their complaint, particularly when the perpetrators operate from different states or outside the country.

Additionally, digital arrest scams frequently rely on temporary communication infrastructures, such as disposable phone numbers, encrypted messaging services, and rapidly created online identities. These technological features significantly complicate the process of identifying perpetrators and collecting admissible evidence. Law-enforcement agencies must therefore develop specialized forensic capabilities capable of tracing digital communication patterns and financial transaction networks. Another critical institutional challenge concerns public trust in digital governance systems. The success of digital arrest scams depends largely on the credibility of the impersonated authority. Fraudsters deliberately exploit the public's respect for institutions such as police departments, financial regulators, and courts. By presenting fabricated documents bearing official logos or by conducting video calls with backgrounds resembling government offices, they manufacture a convincing appearance of legality.

This phenomenon highlights a paradox of digital governance. As states increas[22]ingly adopt online platforms for administrative and judicial processes, citizens become accustomed to interacting with public authorities through digital channels. While such developments enhance efficiency and accessibility, they also create opportunities for malicious actors to replicate official communication formats. Without robust verification mechanisms, ordinary citizens may struggle to distinguish genuine official communication from fraudulent impersonation. Institutional responses must therefore incorporate verification infrastructure that allows citizens to easily authenticate communications purportedly originating from public authorities. Secure digital signatures verified communication portals, and centralized notification systems could play a crucial role in preventing impersonation. If individuals can reliably confirm whether communication originates from a legitimate government source, the effectiveness of digital arrest scams would be significantly reduced.

REFORM PROPOSALS

Digital arrest scams must be combated in a number of ways. First, the law must be more precise. The Australian Parliament, for example, may wish to introduce laws that address the digital impersonation of law enforcement officers, and also include provisions for increased penalties for instances where arrest simulation through psychological coercion occurs.[23] Second, procedural safeguards must be strengthened. In the same way that arrest guidelines were established in *D.K. Basu v. State of West Bengal*,[24] and in various other similar cases, public education campaigns should seek to inform and educate the public on the fact that there are no legal mechanisms for arrest through video conference calls, and also that there are no legal mechanisms for arrest that involve a money transfer to an enforcement agency.

Third, more technological safeguards are needed. It is imperative that telecommunications and digital service providers utilize AI to combat digital fraud by detecting impersonation of law enforcement officers. Furthermore, frameworks on victim compensation should include recognition of psychological damage in addition to economic loss. Damaging effects can be lessened through the establishment of cybercrime reporting portals and account freezing tools. Additionally, it would be constructive for constitutional courts to demonstrate that freedom in

[22] *Supra* note 18.
[23] Vimal Kumar et al., *AI-Powered Ransom Negotiation for Mitigating Cyber Extortion Losses in Digital Arrest Scams*, in 2025 IEEE International Conference on Advances in Computing Research On Science Engineering and Technology (ACROSET) 1, (2025), https://doi.org/10.1109/acroset66531.2025.11280609.
[24] (1997) 1 SCC 416.

the digital age encompasses an absence of technological oppression. This would ease the work of the legislature & executive.[25]

CONCLUSION & A WAY FORWARD

Digital arrest scams painfully illustrate a disturbing intersection of technology, fear and a proxy display of state power. They test the limits between private criminal behavior and state-like coercion. Victims of these scams are psychologically traumatized and held in a state of fear, and compliance that, in effect, resembles unlawful detention. The constitutional guarantee of the right to live with dignity, as a component of the guarantee of personal liberty as contained in Art. 21 of the Indian Constitution, has undergone substantive transformation over the years. If courts are to be serious about the evolution of the thought, then digital arrest scams should be treated as a serious violation of constitutional principles.

Even though private actors were involved, the State's obligations under Art. 21 involve positive concerns about cyber prevention, enforcement, and education. In addition to protection from unlawful physical detention, the State also needs to safeguard against digital engineering detention. With the rapid digital transformation of the country, the growing threats to autonomy will require imaginative developments in the constitutional right to personal liberty. That right must not only be violated in the prison cell or police station but also from the smartphone, the video call, & digital interface, spaces where fear, and authority, and coercion are now prevalent. Only then can Art. 21 of Indian Constitution be a meaningful part of the constitutional right to personal liberty in the 21st century.

[25] Akshay Bhardwaj, *Digital Arrest As An Emerging Offence In India: An Analytical Study*, 6 Int'l J. Rsch. Publ'n & Revs. 3862, (2025), https://doi.org/10.55248/gengpi.06.1125.38139.