DIGITAL ARREST AND ONLINE IMPERSONATION FRAUDS: A JURIDICAL EXAMINATION OF CHANGING DIMENSIONS OF CYBER-CRIME IN INDIA

Parth Malhotra, Sardar Patel Subharti Institute of Law, Subharti University

ABSTRACT

As technology has advanced and communication has shifted to the internet, the face of crime in India has changed significantly and new types of cybercrime have emerged. Digital arrest scams and online impersonation frauds are two of the new threats that have become common. The offences prey on fear, lack of technical knowledge, the trust of the institutions or ignorance of the procedures in order to extort money, steal sensitive data and psychologically manipulate victims. The increased incidents of these offences have revealed significant deficiencies in the Indian legal and enforcement system both in terms of jurisdiction and the evidentiary requirements of the offences. The research explores the juridical view of digital arrest and impersonation frauds in India by examining the existing statutory frameworks and further talks about the role of investigative agencies in addressing these virtual crimes. The study further aims at proposing reforms and strengthening cybercrime enforcement in India.

Keywords: Digital Arrest, Cyber Fraud, Law Enforcement, Impersonation and Cyber-crime.

Introduction

The character of illegal activities has drastically transformed due to the growing financial, administrative and social interactions. Digital Arrest frauds and impersonation-based scams are built on technological and psychological lack of trust. These crimes are typically connected with financial frauds, online crimes, identity thefts and highlights how the traditional method of fraud has morphed into a well-structured technologically sophisticated illegal practice.

In India the term "digital arrest" is not legally defined or entrenched in the legal system, but it has grown in prevalence over the last few years. In these kinds of operations, the scammers would impersonate themselves as representatives of well-known organizations like: Nationalized Banks, the Central Bureau of Investigation, Police and ask for the transfer of funds or confidential financial information from the victim, with the guise of "settlement" or "verification". This kind of deception is a serious misuse of the law, power and legitimacy of the state to compel compliance. Simultaneously, impersonation scams have expanded exponentially which is rendered possible by improvements in communication technology and rising availability of private information. To defraud victims, the cyber thieves pretend to be a number of individuals, including a close friend, family member, employee of the financial institution or law enforcement officer. These crimes are often difficult to be tackled with traditional criminal justice system because of their dynamic and international nature. Both impersonation and digital arrest scams are unique as they use social engineering techniques instead of only advanced ones. These crimes are orchestrated with cognitive biases such as fear, urgency and respecting authority. The use of non-bailable warrants, threats of freezing of accounts or accusations of involvement in more serious crime such as laundering of funds or drug trafficking makes it impossible for the victim to make reasonable decision. The results of these scams indicate an important paradigm shift in the cybercrime world from hacking systems to attacking human resources. According to the government data, the financial scams has caused loss of millions of rupees; and cases have increased by almost three times from 2022 to 2024, from 41,000 to 1,23,000[1]. The scams have become so prevalent that campaigns of digital awareness are created throughout the country.

The journey of India towards a digitally driven economy has been transformative and rapid.

[1] Reserve Bank of India, "Annual Report on rise in digital payment frauds and cyber enabled financial-crimes 2022-2023" (2023)

The mantra of Digital India, the popular Unified Payments Interface and the linking of identity systems like Aadhaar have revolutionised the way citizens interact with the State, financial institutions and other citizens. From banking to taxes, from communicating to governing, today's everyday activities are deeply entrenched in digital platforms. This growth has improved the efficiency, availability, financial inclusion and pulled millions into the formal economy. This fast pivot to digital has also given rise to a parallel ecosystem of vulnerabilities. The same infrastructure that makes it easy to do transactions and govern remotely has created fertile ground for advanced cyber frauds. Fraud is not just about deceptive tactics anymore, but about layered tactics including both technology and psychological manipulation. One of the most alarming trends is the notion of "digital arrest" frauds, where scammers pretend to be law enforcement officers via video calls, fake documents and deceptive methods. The victim is forced to comply by making him or her feel that he is under official investigation or that he or she is about to be arrested. This is a change of the character of criminality from physical control to virtual domination, which involves coercion by means of screens, but incurs real-life economic and psychological damage. What makes the offences so challenging for the legal system is that they are multi-faceted offences, across various disciplines, technology, criminal law, financial regulation and human behaviour[2]. Existing systems of law, established to tackle more 'real world' based offences, can fall short of appropriately describing the nature of these digitally mediated crimes. The technological development and legal readiness of India's digital governance model are clearly showing that there is a growing gap between the two and so it is very important to review and reflect whether current laws and enforcement framework is ready to deal with the growing threat scenario. India's digital infrastructure has also revolutionized the way criminal activities are conducted, making it easier for criminals to carry out their operations while making it more challenging for law enforcement to stop them. Cyber-enabled frauds have grown in size and complexity due to increased use of digital communications platforms and online financial systems.

The difference between digital impersonation and traditional impersonation fraud is the aspect of coercive control. Victims are often threatened not to hang up the phone, to retreat to a secluded place, and to send money as part of a "verification" or "settlement". The threat of legal repercussions, social stigma and on-the-spot arrest puts a person into a "panicky state" which hinders rational decision making. This strategy is an example of a calculated exploitation

[2] Robert B. Cialdini, "*Influence: the psychology of persuasion*" (Harper Business, 2007)

of authority bias: a psychological tendency to obey perceived figures of authority that has long been noted in criminological research.

From a legal perspective, digital arrest scams reveal major weaknesses in current legislation. Jurisdictional, attributional and evidence gathering have become more salient issues when the perpetrators employ anonymisation, encrypted communications and financial networks within the offshore sphere. Digital arrest in this way marks the onset of a new kind of illegality in the digital era. It highlights a need to revisit legal concepts to reflect non-physical manifestations of restraint, the simulation of authority and the need for a more holistic solution that involves legal reform, strengthening of technology and institutions. With the rise of digital communication technology, impersonation frauds in India have become much more sophisticated in terms of nature and execution. Traditionally, impersonation offences were narrow in scope and were typically committed by physically being in the vicinity of the person to be impersonated or by direct interaction with the person. An impersonation, however, has become a very large and technologically advanced type of cybercrime in today's era thanks to the availability of mobile networks, Internet communication service and digital financial systems. Spoofed phone numbers, bulk messaging and Voice over Internet Protocol (VoIP) technologies are frequently used to impersonate through telecom service[3]. Offenders use caller ID spoofing to spoof numbers that look similar to those of a legitimate service provider or government authority. This can be via phone calls or messages claiming that the account has been deactivated, KYC is incomplete, or there's suspicious activity, causing the victim to divulge one-time passwords (OTPs) or other confidential details. This type of fraud also leverages the trust consumers have in telecom infrastructure as a key means of communication, just as banking-related impersonation frauds have surged in tandem with the growth of digital payment processing. Fraudsters often pretend to be bankers, customer care staff or representatives of financial institutions, taking advantage of the trust that these regulated institutions have established. They might ask for account information as part of the verification process, give fake loan approvals or make an urgent call to seem like they're acting in case of unauthorized transactions. The use of real-time payment systems has exacerbated the risk, because once the fraud is pulled off, funds can be transferred to another person in an instant and it's difficult to recover them.

[3] UN office on drugs and crime (UNODC), *Comprehensive study on cybercrime* (2013)

Perhaps the scariest aspect of impersonation fraud is the use of law enforcement identities. In these, the aggressor pretends to be a police officer, an agent of an investigative agency or a member of a regulatory body, and makes contact on the telephone or via video conferencing. The victim is frequently blamed for engaging in serious crimes such as money laundering or other cybercrimes and is threatened with immediate legal action. The illusion of legitimacy of these institutions produces a strong psychological effect which makes it difficult to resist giving instructions to the victim, such as transferring a sum of money or revealing information. This type of impersonation often involves the concept of "digital arrest," in which the impression of custody is created through ongoing monitoring via the Internet[4]. The combination of technology and social engineering, which is very prevalent today, has also made such schemes more effective. The criminals have now got the latest tools at their disposal, including voice cloning with AI, deepfake video interfaces and digital documents created by professionals. The progress of these developments makes it difficult to differentiate between real communication and fake communication and hard for victims to identify deceptions. In terms of the law, impersonation frauds happen in a variety of industries, including telecom, banking, and law enforcement, and reveal significant regulatory shortcomings and criminal law enforcement deficits[5]. Existing laws and rules against identity theft and cheating do not adequately reflect the multifaceted experiences of contemporary impersonation, which involves psychological control as well as technology. This highlights the critical need for a more comprehensive legal and institutional approach to impersonation, viewing it not only as a form of deception but as a complex threat to the integrity and trust of systems.

Deconstructing 'Digital Arrest': Nature and Legal Character

The concept of "digital arrest" is not clearly defined in the law, but rather has become a descriptive term for a new form of coerced activity using digital technology. In essence, digital arrest occurs when a person is induced, through digital communication, to feel that they are lawfully arrested or are about to be arrested by state officials without any physical constraints or legal process. This is a radical departure from the traditional view of arrest, which is fundamentally embedded in physical control, legitimate power and procedural protections[6]. One of the most salient aspects of digital arrest is the exertion of coercion outside of the grasp

[4] Ministry of Home Affairs, Government of India, Advisory on cyber crime frauds including impersonation and digital arrest scams (2023)
[5] *Ibid.*
[6] Telecom Regulatory Authority of India, Consumer Awareness on Telecom Frauds (TRAI, 2022)

of physical custody. The right of the person to be free from personal restraint, whether by force or by any other means, and the requirement to inform the arrested person of the reasons for his arrest, and to produce him before a magistrate, in classic criminal law. Digital arrest, on the other hand, is completely in the virtual world where the victim's freedom is not physically taken from him, but psychologically held. Victims are frequently asked to stay on video calls with the perpetrator and not interact with people and follow the instructions given by the perpetrator, creating a state of "virtual confinement."[7]

Such coercion is very much based on the imposition of the illusion of state power. Usually, the offenders pretend to be from a well-known law enforcement or regulatory agency, employing fake IDs, fake documents and fake environments to create a sense of authenticity. Perpetrators often use video conferencing systems to give the appearance of an official proceeding, and occasionally wear uniforms or use backgrounds of police stations or government offices. When such institutionalism is deliberately reproduced, it is the very respect for and fear of state power that will make compliance and cooperation possible in a digital arrest scam.

In the legal sense, the issue of digital arrest is a complicated one of classification. Elements of several offences, such as cheating, personation, criminal intimidation and extortion, can be satisfied at the same time. But these types are not exhaustive of the special combination of deceit and compulsion that characterizes digital arrest. Digital arrest is not a simple form of cheating, as consent is achieved through deception; it is an extra degree of compulsion that requires for the victim to not wish to go through it because of the threat of legal ramifications. In a similar way, extortion is about extracting property through threats, whereas digital arrest is about intimidating through a mechanism of 'legality' rather than through an explicit threat of harm. This hybridity brings to the fore a conceptual lacuna in the current criminal law structure, including in legislation like the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023. These laws do not speak explicitly to virtual coercive custody, but only to individual elements of the offence, namely identity theft or cheating by personation. Consequently, the provisions might be applied in a piecemeal manner and thus, the seriousness of the offence might be reduced and prosecution be made more difficult for enforcement agencies.

[7] *Ibid.*

Moreover, there is a jurisprudential shift in traditional conceptions of "restraint" and "custody" in connection with digital arrest. The concept of restraint, in legal theory, has usually been linked to bodily restriction from moving. Digital arrest, however, shows that when the psychological domination is strong and convincing and can achieve similar results, that is, a functional equivalent of physical detention. Victim may not seek help, may obey illegal demands, may be emotionally distressed, free of physical restraint. This brings the important question to mind whether the law should embrace the concept of "form of restraint" in criminal law to include non-physical means of coercion[8]. Digital arrest is, in short, a paradigm shift in the manner of coercion in the digital era. It highlights how increasingly adept the bad guys are at wielding perception and authority for compliance without force. The lack of a clear legal system to deal with this phenomenon does not only make enforcing it more difficult, but also presents a real need for doctrinal innovation to tackle the new and emerging forms of cyber coercion.

Conventional cybercrimes usually do not involve pretending to be sovereign or pretending to be an authority figure. What perpetrators do is not just to assume the person's identity, it is to recreate the institutional aura of the State itself. These include the use of fabricated warrants, fake letterheads with official-looking stamps and logos, and props like police uniforms or set-ups that mimic police stations, courtrooms or offices. The goal is to trick and to make the person comply with the order of the State by visualizing him/her through a video call. Such interactions contain a performative element that formal language, procedural terminology and reference to legal provisions further reinforce the illusion of legitimacy. The victims are frequently provided with fake papers or screenshots of a case that appear to be ongoing but are, in fact, false. The victims are presented with fake papers or screenshots of a case that seem to be ongoing but are not. This simulation turns a fraudulent communication into a psychologically coercive environment, which is similar to official proceedings. Such strategies work best by capitalizing on the social set of beliefs about authority that are deeply entrenched in society. The State in legal systems, especially in India, has a coercive role, such as arresting, investigating, prosecuting, etc. These powers can be simulated in a believable way and as a result, people are more likely to follow the orders. The threat of legal sanctions, including arrest, detention or public humiliation, is a strong moral incentive, and will often outweigh

[8] Ministry of Home Affairs, Government of India, Cybercrime Awareness Handbook (2023)

reason[9].

Legally, this behaviour gives rise to challenges in distinguishing the conduct from the existing criminal law. Impersonating a public servant at the first level of abstraction, is a personation offence. But the digital arrest frauds aren't just about impersonation. The final goal is usually the acquisition of money or useful information, and these relate to the crime of cheating. Statutes such as the Information Technology Act, 2000, provide for penalisation of cheating by personation (Section 66D) which is a broad enough definition of cheating to encompass much of the activity of this kind.

Meanwhile, the forceful aspect of it adds some aspects of criminal intimidation and extortion. The perpetrators may threaten to arrest the victim, prosecute him/her, or otherwise cause him or her damage if he/she does not cooperate with them. These are threats that are based on false power, but are felt as real because of the "simulation" of state power. In such a case, the removal of money in such a situation might meet the elements of extortion, which is the delivery of property under the influence of fear. The hybrid nature of the digital arrest is also difficult to understand from a juridical perspective, as it is the case with threats and pressure as well[10]. This is not a clearly defined category of offence, but rather an amalgamation of cheating, impersonation, intimidation and extortion. This multitude renders investigation and prosecution difficult, because the law enforcement has to gather multiple laws to help him or her find a way to tackle one strand of activity. Furthermore, "simulation of sovereign authority" is not specifically mentioned as an aggravating circumstance, which hampers the capacity of the law to reflect the seriousness of the offence. Digital arrest frauds are in essence an example of how the symbolic authority of the State can be appropriated in the digital domain. Replicating official power visually, procedures and language make it very hard to distinguish between deception and coercion. This increases the effectiveness of the fraud and also highlights the shortcomings of available legal structures in dealing with crimes that exploit of the weaknesses of legal systems, authority, tech, and psychological manipulation. The typologies and evolution of online impersonation frauds.

Online impersonation frauds are among the most sophisticated types of fraud, which evolve according to emerging technologies and laws. At the basic level these frauds are the misuse or

[9] *Ibid.*
[10] Tom R. Tyler, "Why people obey the Law" (Princeton University Press, 2006)

falsification of identity for the purpose of defrauding and gaining financial or informational advantage. But the modern world shows a much more complex typology, in which impersonation goes beyond mere identity theft to the creation and manipulation of identity[11]. This is the critical difference between identity theft and identity fabrication, because identity theft is not the only form of impersonation. Identity theft is the use of an existing individual's personal information, like bank details, Aadhaar numbers or login credentials, to impersonate the individual. Identity fabrication, however, involves the development of completely fake identities, which frequently involve the use of fake documents, synthetic online profiles, and digital footprints. Identity theft is based on the use of an existing trust relationship, whereas identity fabrication builds additional levels of credibility, making it harder to detect.

Impersonation frauds can be broadly classified within this framework depending on the intent of the fraud. Frauds that target financial systems, especially banking and digital payment systems, are the most common. Offenders often pretend to be from a regulated financial institution, such as a bank, customer service team or payment processor, to gain trust from their targets. Authorities' impersonation is a more forceful form of impersonation that involves pretending to be an authority figure like a law enforcement or regulatory official. Offenders use the power of institutions like the police or investigative agencies to instil fear and urgency. Persons are frequently made to fear arrest or prosecution and are allegedly forced into a role in illegal activity. In addition, there is a strong overlap with digital arrest scams in which there is a strong focus on psychological control in combination with impersonation[12]. An additional dimension is the use of social engineering, which is used in almost all impersonation scams. Social engineering is defined as the process of using manipulation of human behaviour to gain access to systems that is more related to trusting, fearing, curiosity or urgency and less to technological weaknesses. In recent years, there has been a trend of more hybrid fraud approaches, where multiple methods are used together to improve the fraud's effectiveness[13]. for example, a frauded might start by pretending to be someone else, then threaten to pursue legal action and finally make a claim for money because of a bogus problem. The multiple layers increase the likelihood of the fraud being successful since both cognitive and emotional reactions will be triggered in the victim. It is a reflection of the overall state of cybercrime, where categories of offenses are increasingly becoming more and more indistinct. In a legal

[11] OECD, *Identity theft and misuse of personal data in the digital age* (2019)
[12] *Ibid.*
[13] Kevin D. Mitnick, *The art of deception* (Wiley Publication, 2002)

context, the development of impersonation frauds presents several issues about the effective nature of the current legislative framework. The Information Technology Act, 2000 and similar laws criminalize identity theft and cheating by personation, but do not adequately address multi-stage frauds or 'made up' identities. Likewise, provisions in the Bharatiya Nyaya Sanhita, 2023 cover cheating and impersonation, with a lack of detail in their treatment of technologically-mediated identity construction. It highlights the need for a more refined legal approach which takes into account how the typologies of impersonation are changing in the digital sphere.

Technological Dimensions: AI, Deepfakes and Synthetic Identities

As AI and digital communication technology have rapidly progressed, impersonation fraud by cybercriminals has also improved considerably. Once a simple deception tool, it's now a technologically advanced business that uses AI voice cloning, deepfake video synthesis, encrypted communication networks and more to bolster credibility and avoid detection. AI-powered voice and video cloning technology is one of the most revolutionary advancements in this area. With these tools they can mimic not only the actual words and tone of speech, but also the facial expressions of real people, with considerable realism. In essence, this gives fraudsters the ability to mimic the look of a bank employee, company CEO or even family member. Suspects and victims are less likely to be suspicious when the voice is familiar or authoritative[14]. Very closely related is the development of the deep fake, where fake and highly realistic audio-visual content can be created. In the case of impersonation fraud, a deepfake may be employed to mimic a real encounter with a law enforcement or governmental official through video calls. The visual authenticity of this content contributes to the appearance of the message's legality, making it hard for the victim to tell if a message is legitimate or not. Besides AI-powered tools, cybercriminals use heavy technologies that help to obfuscate and anonymize evidence. Offenders can use caller ID spoofing, Virtual Private Networks (VPNs), and encrypted messaging apps to hide their identities and whereabouts. However, calls may be switched between different jurisdictions (Voice over Internet Protocol (VoIP) services) making it difficult to trace the origin of the calls. The idea of a synthetic identity adds to the technological complexity, which also includes technologies that assist in executing fraud and greatly impeded investigation and prosecution[15]. Synthetic identity theft uses a combination of

[14] Europol, "*Facing reality? Law enforcement and the challenge of Deepfakes*" (2022)
[15] *Ibid.*

true and falsified personal details to create a new identity, as opposed to the traditional identity theft, which utilizes existing personal information. These identities can be true ID numbers with false names or addresses and can get past initial ID checks. Technological developments raise unprecedented challenges on a legal and regulatory level, as such identities can build up very credible digital histories over time. The existing laws such as the Information Technology Act, 2000 were not created to deal with the complexities of deceptive AI or the construction of a fake identity. Likewise, evidentiary laws are unable to keep up with the potential for fabricated digital evidence, and there are questions as to authenticity and reliability in judicial proceedings. In short, technology has not only magnified the amount of impersonation fraud, it has also totally transformed the way in which it is conducted. Impersonation is now a very sophisticated and hard-to-detect mode of cybercrime, with the convergence of AI, deepfakes, and anonymisation tools. This requires refocusing of legal and policy approaches and enforcement methods to be effective in today's complex digital world.

Mapping the Indian Legal Framework: Substantive, Procedural and Regulatory Architecture

There is no single specific dedicated legislation in India for the regulation of digital arrest and online impersonation frauds. Rather, it lies in a multilevel legal structure, in which various components of the offence of identity misuse, deception, coercion, and financial extraction have different yet overlapping laws to address them. This unstructured approach acknowledges the changing face of cybercrime, as traditional legal classifications are being challenged by technologically facilitated behaviour. The Information Technology Act, 2000, is at the top of this framework and is the main statute for cyber offences. Crimes committed through use of a dishonest or fraudulent electronic signature, password or other unique identification feature are subject to Section 66C of the Act. This is pertinent in relation to impersonation frauds when someone obtains personal details like OTPs or digital IDs without permission to impersonate. There is a close link with Section 66D of the same Act, which makes it an offence to cheat by impersonation through the use of computer resources. This covers scenarios where fraudsters use electronic means to pretend to be bank representatives, telecom providers or law enforcement. But it does not adequately reflect the coercive nature that is characteristic of digital arrest scams (such as compliance achieved via fear as opposed to misrepresentation); nor does it cover other aspects of the Act, including Section 72 (concerned with breaches of confidentiality and privacy) or Section 66 (in combination with Section 43) about the

manipulation of data and unauthorised access. The provisions enter into force when personal data is illegally collected and is then used to enable impersonation. In addition, Section 79 sets the principle of intermediary liability; it provides conditional immunity to online platforms provided they can prove that they have taken due diligence measures[16].

The IT Act has dealt with the technical aspects of impersonation while the substantive criminal liability is governed by the Bharatiya Nyaya Sanhita, 2023. This statute is almost always used in conjunction with other provisions in internet arrest fraud. If they are tricked into handing over money or valuable items, then section 318 (cheating) is used. Section 319 (cheating by personation) is available where a person purports to be someone else, in this instance a public body. Coercive aspects of such frauds are also addressed in Section 351, which covers criminal intimidation (including threats to reputation or personal liberty)[17]. If the victim is forced to make the transfer under threat of arrest or prosecution, the action could also be a crime under Section 308, which criminalizes acts of extortion, or the giving of property based on a threat of injury. Also, if false warrants, notices or identification papers are issued, the provisions concerning forgery and the use of falsified papers apply. Along with these sections, a composite crime emerges: digital arrest is not a single crime, but rather a multi-doctrinal crime. But there is no uniform definition included in the statutes and this creates ambiguity and makes it difficult for the prosecutors to build a strategy. Bharatiya Nagarik Suraksha Sanhita, 2023 establishes the procedural mechanism for investigating, prosecuting and adjudicating offences such as impersonation and digital arrest frauds using cyber means. Although the statute is more adaptable in its technological aspects than its predecessor, its application to cybercrime does continue to show structural shortcomings.

Section 173 BNSS requires a First Information Report (FIR) to be filed at the threshold stage in cognizable offence[18]. Cheating, extortion and impersonation are common components of digital arrest scams that must be dealt with by the police. The idea of compulsory registration is very well established in a landmark case where the Supreme Court ruled that the police must register an FIR in case of cognizable offences. This is especially important for cyber frauds, where you may not be able to recover the losses if you delay in the investigation[19]. Further, provisions for search and seizure in sections 94-100 BNSS allow law enforcement authorities

[16] Information Technology Act, 2000, s. 66, 66C, 66D, 72 and 79
[17] Bharatiya Nyaya Sanhita, 2023, s. 308, 318, 319 and 351
[18] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 173
[19] Lalita Kumari v. Government of Uttar Pradesh, (2013) 2 SCC 1

to access and seize relevant material evidence to guide the investigative process. In cyber fraud, this is digital equipment, including mobile phones, laptops, servers and storage equipment. But these rules in digital context have application issues. Unlike physical evidence, the digital evidence is intangible, can easily be copied, and can be deleted remotely, making it more difficult to preserve and seize.

Additionally, the importance of Section 105 BNSS, attachment and forfeiture of property arise in cyber fraud cases as it allows for the freezing of bank accounts and attachment of proceeds of crime. This can be important in digital arrest scams, in which the funds are frequently moved quickly through a variety of accounts, leading to the possibility of asset dissipation. But it takes a long time to bring such powers into play, and in real-time payment systems they often fail to provide an effective remedy[20]. The place of trial is dealt with in Section 185 BNSS, which covers jurisdictions. Cyber offences often cross borders, and can be committed from different states or even abroad. The provision does offer some flexibility, but is not completely ready to deal with the challenges of cross-border cybercrime, which involves a number of issues of extradition and international cooperation. Another vital procedural issue is collection and handling of electronic evidence. The Act acknowledges electronic records as part of the investigation, but does not offer specific procedures for preservation, forensic imaging, or chain of custody, for any particular technology. This often creates evidentiary issues in court, and such issues may result in the exclusion of evidence. Although, the act offers a basic procedural structure, it has limited applicability in combating digital arrest and digital impersonation frauds due to its lack of adaptation to the realities of cyber investigations, which includes the speed of arrests, the coordination of investigations across borders, and the management of digital evidence.

The Bharatiya Sakshya Adhiniyam, 2023 on the other hand, is the legislation which governs the admissibility, relevance and assessment of evidence, including electronic evidence in judicial proceedings. In the context of digital arrest and impersonation fraud, the provisions of this statute are of central importance since there is a significant amount of evidence that is digital. As times change, the Act has sections 61-63 which recognize electronic records as evidence. These include many types of digital information, including email, voice mail messages, video conferencing logs, transaction logs, and digital documents. However, careful enforcement of the procedural protections designed to ensure the authenticity and reliability of

[20] *Supra* note 18, s. 105, 185

the evidence is required for the admissibility. One crucial condition is the certificate for electronic evidence in Section 63 BSA which is in essence a similar condition to the previous Section 65B of the Indian Evidence Act[21]. This certificate should be a confirmation that the electronic record has been taken from a reliable device, and has not been altered. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal the Supreme Court had emphasized that such a certification is necessary for admissibility[22], which was reiterated in Anvar P.V. v. P.K. Basheer.[23]

The requirements ensure that there is greater evidentiary integrity, but also create challenges in cyber fraud cases. The victim will sometimes have to rely on screenshots, call recordings or electronic communications without all the appropriate certification. This may then lead to vital evidence being suppressed on technicalities thereby limiting the prosecution's case. The problems are further exacerbated by the development of deep fake technology and AI-generated content, which is undermining the credibility of digital evidence. Perpetrators could use video calls that have been manipulated or fake documents to pretend to be conducting legal proceedings in digital arrest scams. Advanced forensic analysis is needed to establish authenticity of such evidence, and this is not readily available in the investigative infrastructure. Digital evidence chain of custody is another important issue. Digital Data can be changed easily and can be modified without leaving a visible trail of altering such as physical evidence. Strict adherence to forensic protocols is essential to ensure the evidence presented in court is the same as that is originally collected. The Act also relies on the advice of experts in technical evidence cases. However, the lack of qualified cyber forensic experts and the non-uniformity on how a digital manipulation can be identified makes it even more complex. The Bharatiya Sakshya Adhiniyam, 2023 has recognised and accepted electronic evidence, but the implementation is far from smooth when it comes to arresting individuals digitally and committing impersonation fraud. The legal framework is well formed, but is operating under stress as technology quickly evolves to places where real content is indistinguishable from fake content.

Financial and Regulatory Framework: RBI Norms, Institutional Liability and Systemic Gaps

In India, the financial part of digital arrest and online impersonation frauds is primarily

[21] Bharatiya Sakshya Adhiniyam, 2023, s. 63
[22] (2020) 7 SCC 1.
[23] (2014) 10 SCC 473

controlled by regulatory structures released by the Reserve Bank of India, as the Indian national regulatory entity for banking operations, digital payments, and monetary security. Considering the fact that most impersonation are followed by an unauthorised fund transfer, regulatory requirements on banks and payment intermediaries are key to both prevention and redress. At the heart of this guidance is the RBI Master Directions on Digital Payment Security Controls, 2021, which require regulated entities to adopt comprehensive security protocols such as multi-factor authentication, fraud detection and prevention systems, and transaction monitoring. The Know Your Customer (KYC) Directions provide banks with requirements to confirm the identity of their customers and keep customer records current, while these Directions require banks to implement risk-based transaction monitoring and to identify suspicious transactions, including unusually high dollar transactions. Moreover, the RBI Circular on Customer Liability in Unauthorized Electronic Banking Transactions (2017) provides a framework to decide on the liability of the bank and the customer in the case of electronic fraud. In this arrangement, customers have no responsibility to cover the cost of the unauthorized transaction if it's caused by their bank's carelessness or a problem with the system, provided that it's spotted in a timely fashion. But if the customer consents to move money, like in a digital arrest fraud, the liability is typically with the customer since the transaction is technically "authorized," even if it is a fraud[24]. This poses a big doctrinal and practical problem. Such transactions are regarded as consensual even though the consent is tainted with coercion and deception. As a result, there is a disconnect between what the law says and what victims of Digital Arrest Scams experience; they may find themselves without any financial recourse. Yet another structural constraint is the real-time nature of digital payments, especially those implemented through the Unified Payments Interface (UPI). These systems improve the efficiency, but also allow for instant transfers of funds, giving little room for rescission after the transaction has been done. Banks have come up with schemes like transaction alerts and 'cooling-off' periods, but they are inadequate for situations where lots of money is transferred over several layers in quick succession. Therefore, the RBI regulations bring with it significant compliance burden and enforcement is largely reactive, lacks appropriate compensation structures and cannot effectively respond to frauds based on psychological coercion.

Prevention of Money Laundering Act, 2002: Tracking Proceeds of Cyber Fraud

The Prevention of Money Laundering Act, 2002 (PMLA) is an ancillary but important act to

[24] Reserve Bank of India, *Master Directions on Digital Payment Security Controls* (2021)

deal with the monetary consequences of cyber frauds, such as digital arrest scams. The primary offence is dealt with by criminal law while the PMLA targets the proceeds of crime and their concealment, transfer or incorporation into the financial system. There is a definition of money laundering in Section 3 of PMLA which covers all processes or activities associated with the proceeds of crime, including concealment, possession, acquisition and use. Further, Section 5 PMLA gives the authorities the power to attach property in the name of money laundering which is believed to be involved in money laundering. This can be especially important in cases of cyber fraud where the funds may be dissipated very quickly if bank accounts are not attached promptly[25]. Further, Section 17 gives powers of search and seizure that allow enforcement agencies to gain access to records and financial transactions. Institutional arrangements like the Financial Intelligence Unit-India (FIU-IND) which receive and analyse financial transaction reports such as Suspicious Transaction Reports (STR) sent by banks and financial institutions also play a key role in the Act. While these reports provide a tool to detect unusual patterns that could be associated with laundering of fraud proceeds, the effectiveness of PMLA in cyber fraud cases is constrained by a variety of factors[26]. One of the first reasons is that a digital arrest scam may be a small value, high frequency transaction, which may not meet the value thresholds for reporting as a scam to the regulators. Second, fraudsters often utilize layering methods for moving money from one intermediary account to another, usually the mule account to hide the audit trail. Thirdly, as cryptocurrencies become more prevalent and payment systems such as cross-border payment channels are created, it becomes even more difficult to trace and recover assets in such transactions, which may not be subject to traditional regulatory control. Furthermore, the "game playing" rules and "thresholds" imposed by PMLA may not make it an ideal tool for rapid response in the context of everyday cyber fraud.

Intermediary Regulation: Platform Liability and Due Diligence

Intermediary regulation is a crucial aspect in the legal system, because digital platforms are used to conduct transactions and communicate with each other. It is regulated by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 made under the Information Technology Act, 2000. Due diligence obligations on intermediaries include the appointment of grievance redressal officers, time bound removal of unlawful content on receipt of actual knowledge. Cooperation with law enforcement agencies,

[25] Prevention of Money Laundering Act, 2002, s. 3, 5, 17
[26] Financial Intelligence Unit–India, "Guidelines on Suspicious Transaction Reporting" (2024)

Preservation of information for investigative purposes. Social media intermediaries, and an important class of intermediaries, have been subjected to greater obligations, such as the "first originator" of information in some instances.

These responsibilities apply when: Someone impostors themselves as an official to create a fake profile; Fraudulent messages or video links are sent; Platforms are used to initiate contact with victims of an impersonation or arrest. But the regulatory system is still largely reactive instead of preventative. In Shreya Singhal v. Union of India, intermediaries are only required to take action if they acquire knowledge or lawful orders. That is particularly restrictive on platforms that are able to be held accountable for them failing to proactively detect and prevent impersonation frauds[27]. Furthermore, platforms have no particular need to deploy fraud detection systems based on AI or to detect real-time presence of deep fakes. This is a major regulatory shortfall as it relates to the proliferation of these types of technologies in impersonation scams. One difficulty is the multiple jurisdictions of digital platforms, many of which span multiple countries. Compliance with Indian regulatory requirements may thus be uneven, especially if there is a lack of robust cross-border enforcement. The financial and regulatory system of digital arrest and impersonation frauds shows a multi-institutional yet disjointed system. The RBI offers preventive safeguards, the PMLA offers for tracking of financial transactions after the offences are committed, and the intermediary rules impose responsibilities on platforms; none of these are individually or collectively comprehensive and real-time responses to such frauds. At the heart of the problem is that cyber frauds are moving at a much faster pace than legal and regulatory responses, and are increasingly sophisticated, and so there is a need for integrated, technology-driven and victim-centred reforms.

Comparative Legal Perspective: Evaluating Foreign Frameworks

Foreign law regimes are compared with the US and UK laws, which are more organized, technologically flexible, and focused on enforcement, to tackle cyber enabled frauds such as impersonation and coercion-based frauds similar to the digital arrest scare. These jurisdictions offer more precise statutory classification, effective institutional frameworks and more comprehensive enforcement measures in comparison to jurisdictions such as India where liability is defined by a mixture of general IT Act, 2000 and Bharatiya Nyaya Sanhita, 2023

[27] (2015) 5 SCC 1

provisions.

United States

In the United States, the law is very general and accommodative, giving prosecutors a wide range of anti-cyber laws to use to combat a variety of online crimes. The scope of the Wire Fraud Statute allows for it to be applied to impersonation-based fraud schemes that involve perpetrators using their VoIP, emails, or video conferencing to defraud others. Perhaps more importantly, the statute does not mandate that the fraud be successful; only that there be an intent to defraud along with the use of interstate communication[28]. This is an important reduction in the workload for prosecutors in relation to more limited offenses. Identity misuse is covered by Identity Theft and Aggravated Identity Theft which prohibit the use of fraud in relation to identification documents, authentication features and information. This is a specific focus on the making, holding or use of fake identification, including digital identities. Most important, Aggravated Identity Theft, makes a predicate offence of fraud under the draft legislation a mandatory additional sentence of two years, where id theft is committed in connection with the predicate offence[29]. This represents a legislative recognition that the use of identity is not an incidental but rather a distinct and aggravated harm. In digital arrest scams, criminals impersonate police or government officials, the provisions offer a clear statutory basis for prosecution, whereas the prosecutions under Indian law are more piecemeal. The "coercive" dimension of the digital arrest fraud is addressed with measures like Interstate Communications, which makes it a criminal act to send an interstate communication that contains a threat to kidnap or injure a person. In addition, the United States has laws related to conspiracy under the Conspiracy and RICO Act that criminalize arrangements between at least two individuals to commit an offence[30]. This is significant in cyber fraud cases when the perpetrators are usually a group of operators with callers, data suppliers and financial intermediaries. Authorities can pursue a conspiracy, rather than just individual offenders. Perhaps an even stronger weapon is the Racketeer Influenced and Corrupt Organizations Act (RICO), which enables prosecution of individuals involved in a pattern of racketeering activity as part of an enterprise. Wire fraud is considered a predicate act under RICO. This helps law

[28] Wire Fraud Statute; 18 U.S.C. § 1341
[29] Identity Theft and Aggravated Identity Theft, 18 U.S.C. § 1028
[30] 18 U.S.C. § 875 (Interstate Communications).

enforcement to break up large-scale cyber fraud that can be traced and used to set a pattern of crime[31].

As an institution, agencies like the Federal Bureau of Investigation (FBI) have a key role in cybercrime investigations. The FBI maintains the Internet Crime Complaint Centre (IC3), which is a centralized repository for complaints received from victims, analyses trends, and provides intelligence to law enforcement agencies. The Federal Trade Commission (FTC) complements criminal enforcement by emphasizing consumer protection, and is working to help consumers better understand how to prevent and report fraud[32]. It examines fraudulent practice, issues warnings and can begin civil enforcement proceedings against organisations responsible for fraud. The dual system of criminal and civil enforcement enhances the general regulatory system. One of the major differences between the U.S. system and the rest of the world is the focus on asset recovery and financial tracing. Federal forfeiture laws allow the government to take money earned from illegal acts, whether in the form of a fraudulent payment. This is very important in cases of cyber fraud, where the thing of utmost importance is obtaining monetary benefit. The U.S. system has a high technological level with sophisticated capabilities such as digital evidence analysis, data mining, and surveillance. Police often work with businesses such as banks and computer technology firms, to trace transactions and find perpetrators. This is a joint effort of the public and private sectors which increases preventive and investigatory capacity.

The U.S. system has its drawbacks, though. There has been a range of concerns about surveillance and data collection, especially concerning the Fourth Amendment and civil liberties. Also, there is the issue of jurisdictional issues that can present when there are foreign actors involved, but the scope of the federal statutes is quite broad and can be applied extraterritorially if there is a U.S. communication system or financial channel involved.

United Kingdom

In the United Kingdom, a more formal and specific approach is taken, mainly using the Fraud Act 2006. This act clarifies and adds to the existing legislation that covers many types of fraud by placing them in distinct categories and makes the doctrine more accessible and easier to

[31] Conspiracy and RICO Act, 18 U.S.C. §§ 371, 1961
[32] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3) Reports.

apply. The False Representation component of the Fraud Act, 2006[33] criminalises fraud when a person makes a false representation in a manner that is dishonest with the intention of causing a "loss". This directly applies to impersonation frauds, including those that are done online. Importantly, the offence isn't dependent on any actual loss, with liability for "omissions" and "misuse of trust" under Sections 3 and 4, and preparatory acts under Section 7. This enables the authorities to be involved at an early stage, before the fraud is carried out. Identity related offences are covered in the Identity Documents Act, 2010 which is a criminal offence Act concerning possession and misuse of false identity documents[34]. There is a specific focus on identity-based fraud in this act which further complements the Fraud Act. Regulatory enforcement and financial accountability are also major priorities for the UK. Financial institutions must have a fraud detection system in place and may be under a duty to compensate the wrongdoer in certain circumstances. This makes it a shared responsibility model, where the responsibility is shared and not solely the responsibility of the victim. These agencies work collaboratively and share intelligence, with public awareness campaigns to assist in enforcement[35]. One of the strengths of the UK system is that it is victim-centred and takes into account the coercing and manipulative nature of frauds. The UK system differs from those that regard such transactions as being consensual because it recognises the importance of deception and psychological coerce in destroying consent.

India

The legal framework to deal with digital arrest and online impersonation frauds in India is general and structurally weak and is based on a mix of general criminal law provisions, cyber-specific legislation, procedural rules, and evidentiary rules. Because in India, cyber-enabled frauds are not covered by a single statute, they are dealt with in combination with the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, and procedural and evidentiary statutes. However, it can be flexible and cause problems of doctrinal overlap and doctrinal inconsistencies, especially in cases involving digital arrest scams, where impersonation, deception, and coercion are at play. The substantive offences relating to cyber are largely contained in the Information Technology Act, 2000. Section 66C makes it illegal to use someone else's electronic signature, password, or unique characteristic to cheat in a

[33] 2006, c.35
[34] 2010, c. 40
[35] *Ibid.*

transaction, and Section 66D makes it illegal to cheat by impersonating someone in a transaction using computer resources. These provisions directly apply to online impersonation frauds, such as when the offender pretends to be a law enforcement official or a government official. The extent of these provisions is, however, rather circumscribed, because these provisions are targeted mainly at identity misuse and deception and not sufficiently at the coercive aspect of digital arrest scams[36].

Hence, it is relied on the Bharatiya Nyaya Sanhita, 2023 for the larger criminality involved. The terms cheating, deception for wrongful gain, criminal intimidation, extortion and impersonation are used to encompass the various forms of these offences. Digital arrest scams work by usually causing the victim to fear legal consequences e.g., arrest and prosecution to force them to hand over cash, elevating the actions to a level of extortion and intimidation. Lack of a dedicated offence against digitally mediated coercion, however, means that there is no single offence to prosecute but rather prosecutors are required to assemble multiple offences in order to secure conviction.[37]

As regards the procedure, this investigation and prosecution of such offences is to be regulated by the Bharatiya Nagarik Suraksha Sanhita, 2023 which will deal with the procedure for registering FIRs, search and seizure, arrest and trial. The statute allows law enforcement agencies to pursue cyber-crime, but it is not completely suited to the speed and international reach of digital crime, and funds can be transferred in a flash and criminals may operate internationally. Mechanisms in place e.g., account freezing, inter-agency coordination often have an impact on their effectiveness in the recovery of stolen assets due to delays in implementation[38].

The Indian system, in a way, is an all-encompassing but incomplete answer to digital impersonation, and coercion-based frauds. Existing provisions cover different aspects of the offence, but lack conceptually, technically, and from the victim's perspective. The increasing maturity of digital arrest scams is testament to the need for a more coherent, specialized and future-oriented legal framework to meet the challenges of scams facilitated by the internet.

[36] Information Technology Act, 2000, §§ 66C, 66D.
[37] Bharatiya Nyaya Sanhita, 2023.
[38] Bharatiya Nagarik Suraksha Sanhita, 2023.

Conclusion and Suggestions

The existing regime for digital arrest and online impersonation fraud in India needs to evolve from a disjointed and reactive to a more unified, technology-enabled and victim-centric approach. An immediate reform is the enactment of specific statutory definition of a crime of digital impersonation under the Bharatiya Nyaya Sanhita, 2023 or as a standalone law, in which the third element is coercion and pretending oneself to be an authority. This would remove the existing situation of having several overlapping provisions and give the prosecution a clarity. The Information Technology Act, 2000 is also required to be further strengthened by enhancing the penalties in case the acts involve use of AI tools for impersonation, deepfakes and synthetic identity frauds. There should also be a parallel regulatory mechanism, under the IT Rules, 2021, which will place proactive obligations on intermediaries to deploy automated systems for detecting fraudulent content and impersonation attempts. Similarly, procedural reforms, under the Bharatiya Nagarik Suraksha Sanhita, 2023, are crucial. The use of real-time intervention measures such as locking bank accounts, rapid access to digital evidence and quick-track authorizations for cyber investigations should be recognized in a statutory manner. Such actions would tackle the biggest problem of delay in cyber fraud which can lead to irreparable monetary losses.

Evidentiary matters, on the other hand, will need the Bharatiya Sakshya Adhiniyam, 2023 to be updated to include technology-driven criteria, such as streamlined admissibility of evidence created by victims, acceptance of digital forensic reports and acceptance of tools that use artificial intelligence to determine evidence authenticity. The law should also establish specific presumptions of fact for cases where the content is manipulated, and the crime involves impersonation frauds such as deep fakes. Financial regulatory reforms are needed to create a more “victim-centric” liability system. The Reserve Bank of India should update its guidelines to cover transactions that are made through a deceptive or coerce nature as also effectively unauthorized, thus increasing the scope for compensation to the victim. Banks and payment intermediaries need to be also required to have real-time fraud detection mechanisms and tighter monitoring of mule accounts. From an institutional side, there is a need to strengthen the coordination among various institutions including the Indian Cyber Crime Coordination Centre and CERT-In by creating a fully integrated real-time data-sharing system among the financial institutions, digital platforms and law enforcement agencies. Special focus needs to be given to capacity building in the areas of cyber forensics, AI analysis and cross-border

investigation. Finally, reforms cannot be limited to the law, but also include the measures that are taken to prevent and raise awareness. Digital literacy initiatives that are implemented on a national level, public alert systems and financial institutions and platforms complying with mandated fraud awareness messaging can have a major impact in minimizing victim vulnerability.

To summarize, a strong, technology-enabled and victim-focused approach to digital arrest and online impersonation frauds is needed, as opposed to the current approach, which is fragmented. To achieve preventive and corrective effect, the legal reform should be accompanied by strengthening the institutions, integration of technology and popularization of public awareness. With the dynamic nature of cybercrime, the legitimacy and effectiveness of the legal system will rely on its capacity to be proactive and adaptable, so that the law remains as a means of punishment and also a means of protection in the cyber age.