© Journal of the Indian Academy of Applied Psychology
January 2026, Vol.52, No. 1, 129-137

Digital Arrest in India: An Emerging Psychological Challenges and its Implications for Society

Trayambak Tiwari , Harshita Singh, Anil Kumar Yadav
Banaras Hindu University, Varanasi

Anju L. Singh
Vasanta Kanya Mahavidyalaya, Varanasi

Every facet of human existence, including the legal and law enforcement systems, has changed with the introduction of digital technologies. The term "digital arrest," which describes the limitation of a person's digital activities and access as a kind of punishment or preventive measure, is one of these changes. The rise of digital arrest scams has introduced a complex layer of cyber deception, exploited psychological vulnerabilities and eroded societal trust in digital communication. While the financial and societal implications of such scams are well-documented, their psychological consequences remain underexplored. Victims often experience acute emotional distress, long-term psychological trauma, and a pervasive sense of mistrust. By examining the psychological consequences of these scams, this study seeks to unravel the psychological dimensions of digital arrest scams, providing a conceptual understanding of their impact and exploring potential mitigation strategies for the society.

Keywords: Digital activities, cyber deception, psychological vulnerabilities emotional distress.

The digitization of society has brought forth unprecedented changes in how individuals interact, communicate, and conduct their daily lives. In parallel, law enforcement and governance systems have increasingly incorporated digital tools to monitor, regulate, and enforce compliance. One of the emerging practices in this context is "digital arrest," a term used to describe measures that limit an individual's access to digital platforms, tools, or networks as a means of punishment, prevention, or control. While the concept is relatively nascent, its implications for privacy, human rights, and governance are profound. This paper seeks to explore the theoretical foundations of digital arrest and its broader societal and psychological impact.

Digital arrest can be understood as the restriction or suspension of an individual's digital presence, including access to social media platforms, email accounts, digital financial services, and other internet-based tools (Sharma,2023). It is another increasingly prevalent type of cyber scam in which scammers pretend to be government or law enforcement personnel and threaten victims via audio or video contacts. These criminals frequently pose as law enforcement or other authorities and use fear and anxiety to coerce victims into transferring money or disclosing personal information. The psychological effects of these attacks are profound and appropriate, and they cause victims to feel traumatized, alone, and economically destroyed.

Unlike traditional physical arrests, which involve detaining an individual, digital arrest focuses on incapacitating a person's ability to function within the digital ecosystem. Such measures may be employed as:

Punitive actions, preventive measures, and compliance enforcement are key justifications for restricting internet access. Punitive actions serve as penalties for cybercrimes or online misconduct, including hacking, harassment, or the dissemination of misinformation. Preventive measures aim to mitigate potential harm by suspending accounts associated with terrorist activities, hate speech, or other threats. Compliance enforcement ensures individuals adhere to legal directives, such as court-ordered bans on internet usage, thereby upholding the rule of law in digital spaces.

Theoretical Foundations

Digital arrest can be analysed through several theoretical lenses. Drawing on Michel Foucault's concept of the panopticon, digital arrest reflects a form of disciplinary power in which individuals are constantly surveilled and regulated. The threat of losing digital access acts as a deterrent, encouraging self-regulation and compliance with societal norms. In modern contexts, panopticism is reflected in mass surveillance, data tracking, and workplace monitoring, where individuals alter their behaviours due to the presence of cameras, algorithms, and social scrutiny (Lyon,2023). It remains a crucial concept for understanding power dynamics in contemporary society.

From a social contract perspective, digital arrest can be seen as a mechanism to enforce collective security and order in digital spaces. By agreeing to the terms and conditions of digital platforms, individuals implicitly consent to the possibility of sanctions, including digital arrest, for violating community standards or laws. The application of social contract theory to digital arrest highlights the evolving nature of power and authority in a digital age. It raises fundamental questions: Who enforces laws in cyberspace? What rights do individuals have in digital spaces? And how can we ensure that digital enforcement mechanisms are fair and transparent? As digital governance becomes more prevalent, revisiting the social contract in this new context is crucial for protecting individual freedoms while maintaining order in a highly connected world (Wright, 2022).

Technological determinism highlights how the tools and infrastructure of the digital age shape societal norms and behaviours. Digital arrest underscores the power imbalance between users and gatekeepers of technology, such as governments and tech companies, who control access to digital ecosystems. Technological determinism in digital arrest highlights the growing dominance of automated surveillance and algorithmic law enforcement (Winner, 1977). If technology continues to drive legal and social enforcement without ethical or legal accountability, digital arrests may become an unavoidable feature of modern governance. This raises crucial questions: Can society push back against these technological forces? Or are we inevitably moving towards a future where digital control is the default mode of regulation?

Digital arrest encompasses various forms of cyber exploitation aimed at manipulating, coercing, or defrauding individuals. Financial extortion involves demanding money under threats of fabricated penalties, legal consequences, or reputational harm, often pressuring victims to pay to avoid false accusations or the exposure of private information. Data theft relies on deception or coercion to obtain sensitive personal or financial details through phishing, social engineering, or hacking, leading to identity fraud and financial losses. Prolonged deception, meanwhile, manipulates victims through extended interactions, often using fake identities or emotional manipulation to build trust and extract resources, information, or ongoing compliance.

Psychological Consequences of Digital Arrest

The psychological consequences of digital arrest scams can be both immediate and long-lasting, deeply affecting victims' mental well-being. In the acute phase, individuals often experience intense anxiety, marked by overwhelming fear of legal consequences that may trigger physical symptoms such as rapid heartbeat, sweating, and hypervigilance. The suddenness and shock of being targeted—especially through convincing threats or impersonation of authorities—can lead to cognitive disorientation and disbelief, as victims struggle to comprehend the situation. A profound sense of helplessness often follows, as individuals feel trapped in a scenario they cannot verify or control. Over time, these effects may evolve into more serious mental health conditions. Many victims suffer from post-traumatic stress disorder (PTSD), reliving the experience through nightmares, flashbacks, or heightened alertness, especially when encountering similar online content or interactions. Chronic anxiety and depression are also common, driven by lingering fears of re-victimization, shame over being deceived, and social withdrawal. Perhaps most damaging is the erosion of self-trust—victims often begin to doubt their own judgment, which can undermine their confidence in future decision-making, personal relationships, and digital engagement. This complex interplay of immediate shock and enduring psychological harm underscores the serious emotional toll of digital arrest scams.

Vulnerable populations—including the elderly, individuals with limited digital literacy, and those with pre-existing mental health conditions—are disproportionately impacted by digital arrest scams due to their increased susceptibility to manipulation and difficulty navigating online threats. These groups often experience heightened fear and confusion when confronted with authoritative-sounding threats or complex digital communications, making them more likely to comply with fraudulent demands. The emotional toll can be severe, with many struggling to process the deception and cope with feelings of violation or betrayal. Financial recovery may also be more difficult, especially for those on fixed incomes or without access to support systems. Additionally, the psychological aftermath—such as anxiety, depression, or exacerbation of existing mental health issues—can further hinder their ability to bounce back, leaving lasting emotional and financial scars.

In order to address all forms of cybercrimes in the nation in a coordinated and thorough manner, the Ministry of Home Affairs established the "Indian Cyber Crime Coordination Centre"(I4C) as an associated office. Government is also spreading information regarding digital arrest thorough awareness campaign. Advertisements in newspapers, announcements in Delhi Metros, unique postings created by social media influencers, Prasar Bharti and electronic media campaigns, and a special Aakash Vani program. Many WhatsApp accounts and Skype IDs have been disabled.

The "National Cyber Crime Reporting Portal" (https://cybercrime.gov.in) was established to allow the public to report occurrences related to all forms of cybercrimes, with a particular emphasis on cybercrimes against women and children. In accordance with the law, the State/UT Law Enforcement Agencies in question handle cybercrime events reported on this portal, their conversion into FIRs, and any follow-up actions.

The Central Government has also taken steps to spread awareness on cyber-crime, which include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost),

Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, digital displays on railway stations and airports across, etc (Ministry of Home Affairs, 2021).

Recent cases of digital arrests in India

- Mumbai woman loses Rs 3.8 crore: Cybercriminals impersonating IPS officers and other law enforcement personnel defrauded a 77-year-old Mumbai woman of Rs 3.8 crore. He spent a month in "digital detention" in connection with a fictitious currency laundering case.
- IIT Bombay student loses Rs 7.29 lakh: A student at IIT Bombay lost Rs 7.29 lakh as a result of falling for a "digital arrest" scam in which con artists impersonating TRI police officers stole the money.
- A teacher in Chandigarh loses Rs 51.27 lakh: A 56-year-old educator was defrauded of Rs51.27 lakh by con artists impersonating Mumbai police and CBI officers.
- Between 2023 and 2024, Madhya Pradesh reported a significant rise in digital arrest scams. In 2024 alone, 26 cases were registered, with victims losing over ₹ 12.60 crore—a 130% increase compared to 2023. Authorities have arrested 38 individuals in connection with these scams, recovering approximately ₹ 72.38 lakh. (the Indian express).
- Model Shivankita Dixit from Agra lost ₹ 99,000 after cybercriminals impersonated Central Bureau of Investigation (CBI) officers. They contacted her via WhatsApp, threatened her with arrest, and coerced her into transferring the funds. (Hindustan times)
- A woman in Noida was subjected to a "digital arrest" for five hours and duped of ₹ 1.40 lakh. The scammers impersonated officials and intimidated her into making the payment to avoid supposed legal action.

Ethical and Legal Challenges and Mitigation Strategies

While digital arrest presents a novel mechanism for curbing online misconduct, it introduces a range of ethical and legal challenges that merit serious consideration. The reliance on extensive surveillance to monitor online behaviour raises significant concerns about privacy, proportionality, and the potential misuse of collected data (Lyon, 2017). Moreover, the absence of due process in many digital arrest scenarios—such as opaque account suspensions by social media platforms without clear justification or appeal mechanisms—undermines fundamental principles of fairness and justice (Gillespie, 2018). The restriction of digital access also threatens to deepen existing social inequalities, disproportionately affecting marginalized groups and infringing upon digital rights such as freedom of expression and access to information (Eubanks, 2018). Compounding these issues are jurisdictional ambiguities; the transnational nature of the internet means that actions by authorities in one country can have unintended legal or diplomatic consequences in others, complicating enforcement and raising concerns about sovereignty and accountability (Kuner, 2013).

Counselling and therapy play a vital role in supporting victims of digital arrest, offering essential tools to process trauma, restore emotional stability, and rebuild a sense of personal agency. Individual therapy is particularly important, as victims often struggle with intense feelings of paranoia,

self-doubt, and symptoms of post-traumatic stress—especially when the digital arrest involves impersonation by authorities or public exposure. Therapists trained in cyber trauma and digital harassment can provide targeted interventions to help individuals make sense of their experience and begin healing. Cognitive Behavioural Therapy (CBT) is especially effective in managing anxiety, stress, and negative thought patterns brought on by the sudden loss of digital connectivity, financial insecurity, or social isolation. Recognizing that not all victims have access to traditional in-person therapy, the integration of online mental health resources—including crisis hotlines, virtual therapy sessions, and AI-powered chatbot support—ensures timely and accessible care. Moreover, given the often-complex intersection of psychological harm and legal confusion in digital arrest cases, a multidisciplinary approach is beneficial. Legal-psychological hybrid counselling combines mental health support with legal guidance, allowing victims to better understand their rights, explore recourse options, and reduce the emotional toll of navigating legal ambiguity. This comprehensive therapeutic framework is critical to fostering recovery and resilience in an increasingly digital world.

Peer support groups offer a critical lifeline for individuals affected by digital arrest, addressing the profound sense of isolation and disempowerment that often accompanies such experiences. These groups foster a sense of community and shared understanding, providing victims with emotional validation and practical coping strategies. Secure online and offline support communities—such as encrypted messaging platforms or moderated forums—create safe spaces where individuals can openly share their experiences without fear of surveillance, judgment, or retaliation. Within these spaces, guided support circles led by trained therapists or facilitators offer a more structured environment, allowing participants to discuss emotional recovery, techniques for managing anxiety, and steps for regaining their digital reputation or financial stability. Beyond emotional support, some peer groups evolve into advocacy networks, mobilizing collective action to challenge the legitimacy of certain digital arrests. These networks often engage in awareness campaigns, legal advocacy, and policy lobbying, helping to spotlight cases of abuse or overreach while empowering victims to reclaim their voice. By blending emotional healing with community resilience and activism, peer support groups play a pivotal role in helping individuals recover from the psychological and social fallout of digital arrest.

Awareness campaigns are a crucial preventive strategy in combating the psychological and social harm caused by digital arrest, equipping individuals with the knowledge and resilience needed to navigate an increasingly complex digital environment. Educational initiatives form the foundation of these campaigns, teaching the public about algorithmic biases, digital coercion tactics, online scams, and the implications of unjust digital restrictions. Delivered through accessible channels such as social media, webinars, and interactive workshops, these programs aim to reduce vulnerability and empower users with critical thinking skills. Complementing this are digital hygiene trainings that educate individuals on how to safeguard their online identities, minimize reputational risks, and navigate appeals processes when facing wrongful account suspensions or censorship. Ethical tech advocacy is another pillar, urging technology companies and policymakers to design enforcement mechanisms that are transparent, just, and considerate of users' mental health. Finally, media coverage and real-life case studies of digital arrest victims

help personalize the issue, raising public empathy while generating pressure for systemic reform. Together, these components create a robust framework for both individual empowerment and collective action, fostering a digitally aware and psychologically resilient society.

Mental health professionals serve as first responders to the psychological trauma inflicted by digital arrest scams. Their role begins with providing immediate psychological first aid to help victims stabilize emotionally. This includes creating a safe space for the victim to express their fears and anxieties without judgment. Therapeutic interventions such as cognitive behavioural therapy (CBT) are effective in helping individuals reframe irrational guilt or fear stemming from the experience. Trauma-focused approaches may also be necessary for those exhibiting symptoms of PTSD (Bisson et. al, 2015). In addition, counsellors can assist victims in re-establishing trust—both in themselves and in the systems around them. Many victims report a sense of betrayal, not just by the scammers, but by their own instincts and decisions. Restoring self-confidence and emotional balance is critical for full recovery.

Mental health professionals can also play a significant role in prevention by educating the public on the psychological tactics used in digital arrest scams. Collaborating with law enforcement, schools, colleges, and media outlets, they can conduct workshops and awareness campaigns that focus on digital literacy, emotional resilience, and the importance of critical thinking in high-pressure situations. Teaching people how to identify manipulation techniques and regulate their emotional responses to fear-based threats can reduce vulnerability (Rege, 2020). Furthermore, they can work closely with vulnerable populations—such as the elderly, students, and those with pre-existing anxiety or isolation—to build psychological defenses against such scams. Group therapy and support groups can also be instrumental for victims to share experiences and collectively process their trauma.

Mental health professionals are uniquely positioned to advocate for policies that acknowledge the psychological component of cybercrime. By collaborating with cybersecurity experts, law enforcement, and policymakers, they can contribute to frameworks that provide victims with access to psychological care as part of official support services. Ensuring that psychological counselling is integrated into cybercrime response units and helplines can help victims recover faster and reduce the long-term societal impact of such scams. Moreover, mental health input is valuable in training police and cybercrime officials to handle victims with empathy and sensitivity, as initial responses often determine whether victims will continue to seek support.

Implications for the Society

The concept of digital arrest carries profound implications for justice, social participation, and the role of private actors in governance. By shifting the locus of punishment from the physical world to the digital realm, digital arrest redefines how societies understand and administer justice, highlighting the increasing centrality of online spaces in everyday life. This evolution challenges traditional frameworks of punishment and rehabilitation, prompting a need to reassess how digital sanctions align with principles of fairness and human dignity. Furthermore, restricting access to digital platforms can severely curtail an individual's ability to engage in civic life, from participating in public discourse and political debates to accessing government services, education, and employment opportunities. Such limitations risk deepening social exclusion and marginalization, especially for those already on the fringes of digital

inclusion. Compounding these issues is the prominent role of technology companies in implementing digital arrests—through account suspensions, content takedowns, or algorithmic monitoring—effectively placing immense power in the hands of private corporations. This raises critical concerns about transparency, due process, and accountability, as these companies often operate outside traditional legal frameworks, yet wield significant influence over users' rights and freedoms in the digital age.

To effectively address the complex challenges posed by digital arrest, a multifaceted response grounded in legal, ethical, and educational principles is essential. First, establishing clear legal frameworks is crucial—governments must develop transparent, consistent, and rights-respecting regulations that define the scope and limitations of digital arrest, ensuring it is applied fairly and proportionally rather than arbitrarily or discriminatorily. Alongside this, mechanisms to enhance accountability are vital, particularly concerning the role of private tech companies. These platforms should be subject to independent oversight, with accessible appeal processes to prevent unchecked power and protect users from unjust digital sanctions. Safeguarding digital rights must also remain a top priority; even in cases involving misconduct, individuals should retain fundamental freedoms such as expression, access to information, and participation in digital society. Finally, promoting digital literacy can play a preventative role by empowering individuals with knowledge of their rights, the implications of their online behaviour, and how to safely navigate digital environments. Together, these measures foster a more just, secure, and inclusive digital ecosystem where enforcement mechanisms are balanced with respect for individual dignity and freedom.

Conclusion

Digital arrest is a complex and multifaceted concept that reflects the growing intersection of technology, law, and society. While it offers a novel approach to addressing online misconduct, its ethical, legal, and societal implications must be carefully considered. By situating digital arrest within broader theoretical and practical frameworks, this paper highlights the need for balanced and equitable approaches to governance in the digital age. As technology continues to evolve, so too must our understanding of justice, rights, and responsibilities in an increasingly digital world. Digital arrest scams exploit psychological vulnerabilities, leaving victims with profound emotional and mental health consequences. Understanding these impacts is crucial for developing effective support mechanisms and preventative measures. By fostering awareness, resilience, and psychological support, society can mitigate the harm caused by such cybercrimes and empower individuals to navigate the digital landscape with confidence.

References

Bisson, J. I., Cosgrove, S., Lewis, C., & Roberts, N. P. (2015). Post traumatic stress disorder. *BMJ*, 351, h6161. https://doi.org/10.1136/bmj.h6161.

Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press.

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Pantheon Books.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.

Lyon, D. (2006). *Surveillance Studies: An Overview*. Polity Press.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

Habermas, J. (1984). *The Theory of Communicative Action, Vol. 1: Reason and the Rationalization of Society*. Beacon Press.

Hindustan Times. (2024, December 5). *Former Miss India winner put under digital arrest for 2 hours, loses ¹ 99,000*. https://www.hindustantimes.com/india-news/former-miss-india-winner-put-under-digital-arrest-for-2-hours-loses-rs-99000-101733381474858.html .

Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.

Ministry of Home Affairs, Government of India. (2021). *Indian Cyber Crime Coordination Centre (I4C)* [Press release]. Retrieved from https://www.mha.gov.in/notifications/indian-cyber-crime-coordination-centre-i4c.

National Herald. (2024, December 10). *You are under digital arrest: what you need to know about this scam*. https://www.nationalheraldindia.com/national/you-are-under-digital-arrest-what-you-need-to-know-about-this-scam .

NDTV. (2024, December 11). *Noida Woman Kept Under 'Digital Arrest' For 5 Hours, Duped Of Rs 1.40 Lakh*. Retrieved from https://www.ndtv.com/noida-news/noida-woman-kept-under-digital-arrest-for-5-hours-duped-of-rs-1-40-lakh-7221870.

News18. (2024, April 10). *Mumbai woman loses Rs 3.8 crore: Cybercriminals impersonating IPS officers and other law enforcement personnel defraud 77-year-old*. https://www.news18.com/india/mumbai-woman-loses-rs-3-8-crore-cybercriminals-impersonating-ips-officers-and-other-law-enforcement-personnel-defraud-77-year-old-8876544.html.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Rege, A. (2020). Cybercrime victimization and the role of awareness programs: A multidisciplinary approach. *Journal of Cybersecurity Education, Research and* Practice, 2020(1), Article 5. https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss1/5.

Sharma, R. (2023). *Understanding digital rights and restrictions in the modern age*. Journal of Cyber Law and Policy, 12(3), 145–162.

The New Indian Express. (2024, December 17). *People in Madhya Pradesh lost 130 per cent more money due to digital arrest in 2024 compared to 2023*. Retrieved from https://www.newindianexpress.com/nation/2024/Dec/17/people-in-madhya-pradesh-lost-130-per-cent-more-money-due-to-digital-arrest-in-2024-compared-to-2023 .

Times of India. (2024, November 27). *IIT-Bombay student loses Rs 7 lakh to 'digital arrest scam': 'WhatsApp call from TRAI employee' and more, how he was duped*. Retrieved from https://timesofindia.indiatimes.com/technology/tech-news/iit-bombay-student-loses-rs-7-lakh-to-digital-arrest-scam-whatsapp-call-from-trai-employee-and-more-how-he-was-duped/articleshow/115718034.cms.

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.

Winner, L. (1977). *Autonomous technology: Technics-out-of-control as a theme in political thought*. MIT Press.

Wright, M. J. (2022). Digital sovereignty and the social contract: Rethinking power and authority in cyberspace. In K. A. Patel & S. R. Chen (Eds.), *Governance in the*

Digital Age: Law, Society, and Technology (pp. 87–110). Routledge.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Acknowledgement : Authors wish to acknowledge the partial financial support received from ICSSR, New Delhi and partial support received from IoE, BHU vide Development scheme No. 6031(A).

Trayambak Tiwari, Associate Professor and Corresponding Author, Cognitive Science Laboratory, Department of Psychology, Banaras Hindu University, Varanasi, India. Email: trayambak@bhu.ac.in ; Orcid id: 0000-0001-6047-9701

Harshita Singh, Ph.D. scholar and Corresponding Author, Cognitive Science Laboratory, Department of Psychology, Banaras Hindu University, Varanasi, India. Email: harshitastwinky@gmail.com

Anil Kumar Yadav, Assistant Professor and Corresponding Author, Cognitive Science Laboratory, Department of Psychology, Banaras Hindu University, Varanasi, India. Email: anilyadav@bhu.ac.in

Anju L. Singh, Associate Professor and Corresponding Author, Department of Psychology, Vasanta Kanya Mahavidhyalaya, College admitted to the privileges of Banaras Hindu University, Kamachha, Varanasi, India. Email: anjubhu@gmail.com