Library Progress International *Print version ISSN 0970 1052*
Vol.44, No.4, Jul-Dec 2024: P. 169-172 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

The Psychological Impact of Digital Arrest on Individuals: A New Threat to The Society

Dr. Rajnish Bishnoi[1*], Dr. Pooja[2], Varnika Siyag[3], Rajvir Kaur[4]

[1]Assistant Professor (HoD), Faculty of Law, Guru Kashi University, Talwandi Sabo, Bathinda
[2]Assistant Professor, Department of Law, Punjabi University Regional Centre, Bathinda,
[3]Assistant Professor, Shri Khusal Das University, Hanumangarh
[4]Assistant Professor, Faculty of Law, Guru Kashi University, Talwandi Sabo, Bathinda
***** Corresponding Author, rajnishbishnoi1989@gmail.com

How to cite this article: Dr. Rajnish Bishnoi, Dr. Pooja, Varnika Siyag, Rajvir Kaur (2024). The Psychological Impact of Digital Arrest on Individuals: A New Threat to The Society. Library Progress International, 44(4), 169-172

Abstract

Digital Arrest, the newest form of cybercrime, has emerged as a serious threat to individual well-being and social stability. This article examines the psychological impact of digital violence, examining the emotional distress, psychological distress and behavioural changes experienced by victims It explores the underlying mechanisms by which digital violence can produce profound psychological effects difficult results, including anxiety, depression, trauma. There is post -stress disorder and more, of digital arrest in the article. It discusses social implications, such as loss of confidence a have in institutions, increased social isolation, and economic loss A multi-pronged approach to mitigating the negative effects of digital arrest is proposed, including public awareness, law enforcement response, technical solutions and psychological support for victims and the public from this We can develop effective strategies so that they are protected from the impending disaster.

Keywords

Digital Arrest, Cybercrime, Psychological Impact, Anxiety, Depression, Social Isolation, Mental Health, Public Awareness

Introduction

Accelerating technology has changed the way we live, work and interact. But this digital revolution has also opened up new avenues for crime and exploitation. One such emerging threat is digital arrest, a form of cybercrime in which individuals are coerced or manipulated into transferring funds or compromising sensitive information under the threat of legal action or socially exclusionary This article examines the psychological effects of digital censorship on individuals to, under this emerging threat of implications for multi-faceted society and examines.

Digital Arrest

Digital arrest is a relatively new phenomenon, using technology to intimidate and manipulate individuals into complying with the demands of cybercriminals. Digital arrest is another growing form of cyber scam where fraudsters pose as law enforcement or government agency employees, and threaten victims with audio/video calls. These criminals often masquerade as law enforcement or other authorities, using fear and anxiety to coerce victims their aggression leads to transferring money or sharing personal information psychological impact the of such attacks to be profound Appropriate, and make victims feel traumatized, isolated and economically destroyed.

Recent cases of digital arrests in India

- Mumbai woman loses Rs 3.8 crore: A 77-year-old woman from Mumbai was duped of Rs 3.8 crore by cyber criminals posing as IPS officers and other law enforcement officials. He was held in "digital detention" for a month in a fake currency laundering case.
- IIT Bombay student loses Rs 7.29 lakh: An IIT Bombay student fell victim to a "digital arrest" scam, where fraudsters posing as TRI policemen lost Rs 7.29 lakh.
- Chandigarh teacher loses Rs 51.27 lakh: A 56-year-old teacher was duped of Rs 51.27 lakh by fraudsters posing as CBI cops and Mumbai police.

Psychological Effects of Digital Arrest

The psychological effects of digital arrest can be far-reaching and long-lasting. Victims often experience emotional distress: -

- **Fear and anxiety:** The constant threat of legal influence and social stigma can increase anxiety and fear. Victims worry about the impact it could have on their reputations, careers and relationships.
- **Shame and humiliation:** Victims can feel deep shame and humiliation, especially if they have been publicly exposed or ridiculed. This can lead to shame, guilt, and self-blame.
- **Depression and self-esteem:** Economic distress, social isolation, and emotional turmoil associated with digital lockout can lead to depression and low self-worth Patients struggle with feelings of hopelessness, helplessness and worthlessness.
- **Post-Traumatic Stress Disorder (PTSD):** In extreme cases, victims may develop PTSD, characterized by intrusive thoughts, retrospectives, them excessive alertness and may have difficulty falling asleep, excessive arousal, and avoidance behaviours.
- **Loss Of Trust:** The trust given by cybercriminals can erode victims' trust in others, making it difficult to build healthy relationships. Victims may be wary of online communication and hesitant to share personal information.

Societal Implications

The psychological impact of digital imprisonment extends beyond the individual victim and affects society as a whole. Social determinants include:

- **Loss of trust in institutions:** Frequent incidents of digital piracy can undermine public trust in law enforcement and other institutions.
- **Increased isolation:** Victims may withdraw from social interactions, for fear of further victimization or judgment.
- **Economic losses:** Digital disruption can cause significant economic losses for individuals and businesses, affecting the entire economy.
- **Increased cybercrime:** As cybercriminals become more active, the frequency and severity of digital incidents may increase, posing a greater threat to society.

Challenges of Digital Arrests

Digitalization, a relatively new phenomenon, has emerged as a serious threat to individual privacy, security, and quality of life. These types of cybercrimes, which often involve sophisticated sociotechnical techniques, present enormous challenges to individuals and law enforcement agencies.

Technical Challenge

- **Anonymity and traceability:** Cyber criminals often use elaborate methods to mask their identities, making their activities difficult to trace and bring to justice. This anonymity through anonymity networks, proxy servers and virtual private networks (VPNs) to mask the true origin of a cyberattack.
- **Rapidly evolving technologies:** The rapid pace of technological advances presents constant challenges for law enforcement agencies. Cybercriminals are rapidly adopting new technologies such as artificial intelligence (AI), machine learning and others to enhance their capabilities and evade detection. This requires law enforcement to constantly adapt and invest in cutting-edge technologies in.

- **Cross-border cybercrime:** The global nature of the Internet complicates tackling cybercrime across national borders. Jurisdictional issues, legal frameworks, and disparate cooperation across jurisdictions can hinder effective investigations and prosecutions.

Legal challenges

- **Jurisdictional Issues:** Determining the appropriate jurisdiction to deal with cybercrime can be complicated, especially when victims and perpetrators are located in different countries international cooperation and treaty donor diversification is critical to addressing these challenges, but legal challenges and political considerations often impede progress.
- **Changing Legal Systems:** Legal and technological advances may not always keep pace, creating legal gray areas that can be exploited by cybercriminals. As technology advances, so must legal frameworks designed to combat cybercrime. Lawmakers and policymakers need to work closely with law enforcement specialists and cybersecurity experts to ensure laws are up-to-date and effective.
- **Digital Evidence:** Collecting and presenting digital evidence in a legally acceptable format can be complex and time-consuming. It is important to ensure the integrity and authenticity of digital evidence, as it can easily be tampered with or altered. There is a need to develop standardized methods for collecting, storing and analyzing digital evidence to ensure its admissibility in court.

Mitigating the Impact

A multi-pronged approach is needed to mitigate the negative effects of digital censorship:

- **Public Awareness and Education:** Increased public awareness of the techniques used by cybercriminals could help deter individuals from committing this type of fraud. Educate people on good cybersecurity practices, such as strict password hygiene, avoiding suspicious links, and being cautious about sharing personal information online.

- **Strengthening legislative response:** Law enforcement agencies must be adequately equipped to investigate and respond to digital crimes. Establishment of specialized agencies to tackle cybercrime and stay updated on the latest techniques used by cybercriminals. Cooperate with international law enforcement agencies to dismantle transnational cybercrime networks.

- **Develop effective prevention strategies:** Implement strong cybersecurity measures such as strong passwords, two-factor authentication, and regular software development. Implementing advanced security technologies such as firewalls and antivirus software to protect devices and networks. To encourage organizations to adopt stronger cybersecurity policies and procedures.

- **Provide psychological support to victims:** Access to psychosocial interventions can help victims cope with the emotional trauma associated with digital mind control. Provide counselling and therapy to address anxiety, depression and PTSD. Providing support groups for victims to connect with others who have experienced similar trauma.

- **International Collaboration:**
  Collaborative efforts between countries can help dismantle criminal networks and bring cybercriminals to justice. Sharing information and best practices to combat cybercrime globally. Development of international legal frameworks to combat cybercrime and the extradition of cybercriminals.

National and International laws on Digital Arrest:

International laws and treaties:

Convention on Cybercrime: This international treaty provides a framework for international cooperation in the investigation and prosecution of cybercrime.

Budapest Convention on Cybercrime: This convention covers specific offenses related to cybercrime, including hacking, identity theft and child pornography.

State-specific rules:

United States of America:

- Computer Fraud and Abuse Act (CFAA): This law prohibits tampering with computer systems and networks.
- Electronic Communications Privacy Act (ECPA): This law protects electronic communications, including email and online messaging.

United Kingdom:

- Computer Misuse Act 1990: This act covers computer crimes including hacking, unauthorized access and malicious communications.

India:

- Information Technology Act, 2000: This Act regulates cybercrime in India and provides for offenses such as hacking, identity theft and online bullying.

Conclusion

The psychological impact of digital violence is a serious and growing concern. By understanding the complex factors that contribute to this issue, we can develop effective strategies to reduce its impact on individuals and society. As technology continues to evolve, it is important to remain vigilant and adapt to the ever-changing cybercrime landscape. Working together, we can create a safe and secure digital future.

A multi-pronged approach is needed to address the challenges posed by the digital prison. This includes raising public awareness, strengthening law enforcement capacity, developing strong cybersecurity measures, providing psychological support to victims, and enhancing international cooperation Through these measures using it, we can work towards a future in which individuals are protected from psychological and economic harm through digital imprisonment.

References and Citations:

1. American Psychological Association (APA). (2023). Studies on anxiety and PTSD linked to cyber-related trauma. Link
2. Cyber Psychology, Behavior, and Social Networking Journal. (2023). Insights into psychological effects of cyber threats.
3. National Alliance on Mental Illness (NAMI). (2023). Resources for anxiety, depression, and PTSD associated with digital crimes. Link
4. Trauma-Informed Care Practices. (2023). Mental health interventions for victims of cyber-related trauma.
5. Mumbai Mirror. (2023). Mumbai woman loses Rs 3.8 crore in digital arrest scam.
6. Indian Express. (2023). IIT Bombay student scammed of Rs 7.29 lakh.
7. Hindustan Times. (2023). Chandigarh teacher duped of Rs 51.27 lakh by cybercriminals.
8. Budapest Convention on Cybercrime. (2001). Framework for international cooperation on cybercrime. Council of Europe Link
9. Computer Fraud and Abuse Act (CFAA) (USA). Overview of federal laws against cybercrime.
10. Information Technology Act, 2000 (India). Comprehensive legal response to cybercrime.
11. Computer Misuse Act 1990 (UK). UK law addressing unauthorized computer access.
12. Interpol Cybercrime Reports. (2023). Cross-border challenges in combating cybercrime. Link
13. Norton Cyber Safety Insights Report. (2023). Public awareness on cybersecurity best practices.
14. National Cyber Security Centre (NCSC) (UK). Guidance on improving organizational cybersecurity measures. Link
15. Oxford Internet Institute. (2023). Studies on AI and machine learning in cybercrime.
16. World Economic Forum (WEF). (2023). Collaborative efforts against global cyber threats. Link
17. Convention on Cybercrime (Budapest Convention). International treaty for tackling cybercrime.
18. Cybersecurity and Infrastructure Security Agency (CISA) Resources
19. Cyber Safety Tools and Resources by Norton
20. Council of Europe Cybercrime Division