ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]

VOLUME 3 AND ISSUE 1 OF 2024

APIS – 3920 – 0007 | ISSN - 2583-7230

Published by

Institute of Legal Education

https://iledu.in

A NEW GENRE OF CYBERCRIME – DIGITAL ARREST

AUTHOR - YOGESH PRASAD KOLEKAR, ASSISTANT PROFESSOR AT M.K.E.S COLLEGE OF LAW

BEST CITATION - YOGESH PRASAD KOLEKAR, A NEW GENRE OF CYBERCRIME – DIGITAL ARREST, ILE MULTIDISCIPLINARY JOURNAL, 3 (1) OF 2024, PG. 210-212, APIS – 3920-0007 | ISSN - 2583-7230.

ABSTRACT

Technological advancement serves as a symbol of human progress and advancement. It is often viewed as a tale of growth. The advent of the Internet has effectively transformed the world into a global village, enabling individuals to connect with each other through a device and app/software. In 1996, the United Nations Commission on International Trade Law (UNCITRAL) introduced a model law on Electronic Commerce to provide legal recognition to electronic records and transactions conducted electronically. India enacted the Information Technology Act, 2000 is based on the model law on Electronic Commerce. The emergence of new technology, especially the internet, gave birth to new type of crime known as cybercrime or online offenses. In recent years, a new genre of cybercrime have emerged and created havoc in lives of innocent citizen who fearing arrest fall into the traps of cyber criminals through 'digital arrest'. A digital arrest is a cybercrime where a person personates as a law enforcement officer and intimidate to take legal action or arrest for the offense which the person has actually not done.

Introduction

Technological advancement serves as a symbol of human progress and advancement. It is often viewed as a tale of growth. The growth and development in the field of Information and Communication Technology has transformed and simplified method of human interaction. It has created a global network that can connects individuals across the world. Information technology has revolutionized our methods of learning, voting, working, and entertainment. However, even before effective rules and regulations could be established, the cybercrime has spread its network.

Cybercrime, a term derived from the combination of "Cyber" and "Crime," refers to illegal activities conducted over the internet or in cyberspace. It is noteworthy that the first legislation addressing cyberspace, the Information Technology Act of 2000, primarily focused on issues related to e-commerce, e-governance, and electronic records, with insignificant provision on cybercrime, as evident from its objectives and provisions.

The advent of the Internet has effectively transformed the world into a global village, enabling individuals to connect with each other through a device and app/software. Today people can communicate, see, and share emotions, often providing a more immersive experience enhanced by various GIFs and emoji's. This development has significantly reduced the need for travel, allowing individuals to learn, access information, and sign legally recognized online contracts.

United Nations Commission on International Trade Law

In 1996, the United Nations Commission on International Trade Law (UNCITRAL)[285] introduced a model law on Electronic Commerce to provide legal recognition to electronic records and transactions conducted electronically. The primary aim of this model law was to ensure equal treatment for electronic transactions on par with paper based transaction. India enacted the Information

[285] https://uncitral.un.org/

Technology Act, 2000[286] is based on the model law on Electronic Commerce.[287]

The Information Technology Act of 2000 provides legal framework which acknowledges and facilitates modern technological transactions, including e-commerce, e-governance, electronic records, and digital signatures. The primary aim of the Act was to legalize paperless transactions, placing them on an equal footing with traditional paper-based transactions. The Information Technology Act of 2000 originally contained minimal punitive measures curbing cybercrime.

Cybercrime

The field of Information and Communication Technology has revolutionized human society by establishing a new world known as the virtual world. The emergence of new technology, especially the internet, gave birth to new type of crime known as cybercrime or online offenses. Cybercrime refers to illegal activities conducted through computers or mobile devices, either as tools for committing crimes or as targets themselves. The motivations behind cybercrime vary among individuals, but several common reasons include:

1) Financial gain
2) Theft of data or information
3) Acts of terrorism or disruption
4) Defamation
5) Revenge

The prevalence of cybercrime is both widespread and disruptive, as evidenced by global and national statistics. It is estimated that cybercrime could result in damages amounting to $9.5 trillion USD worldwide by 2024, which would make it comparable to the world's third-largest economy.[288]

According to the Indian Cyber Crime Coordination Centre (I4C), an alarming average of 7,000 cybercrime complaints were reported daily, reflecting a staggering 60% increase from 2022 to 2023.[289] The scale of cybercrime is concerning on both global and national levels, especially as India has emerged as the country with the second-highest number of internet users in the world.[290]

Digital arrest – A new genre of cybercrime

In recent years, a new genre of cybercrime have emerged and created havoc in lives of innocent citizen who fearing arrest fall into the traps of cyber criminals through 'digital arrest'. A digital arrest is a cybercrime where a person personates as a law enforcement officer and intimidate to take legal action or arrest for the offense which the person has actually not done. The cybercriminals tricks the victim to believe that a wrongful act has been conducted by misuse of his or her identity like pan card or aadhar card etc.

A prevalent method is creating a deception that a crime has occurred and other individual is under suspicion of doing it. The victim is kept under observation digitally or virtually for the purpose of investigation and the meantime the victim the coerced to transfers the amount asked by the cyber criminals.

A prevalent practice by cybercriminals in case of digital arrest is seen that these cybercriminals generally use terms which headlines in newspaper like Enforcement Directorate (ED), CBI, MDMA, and money laundering etc to make their narration look actual. Digital arrest is a method of cheating through personation i.e to adopt another person's identity with the intent to deceive or cheat. The imposter generally poses as a police officers of higher rank from narcotics department or other law enforcement agency like ED or CBI.

[286] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[287] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
[288] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/
[289] https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html
[290] https://explodingtopics.com/blog/countries-internet-users

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 3 AND ISSUE 1 OF 2024
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in

Types of allegation

In digital arrest generally following types of allegations are levied which are of serious nature,

Drug related

Money laundering

Misuse of aadhaar or personal ID in serious offense

The victim is made to believe that his personal identity like aadhaar or pancard has been found to be used in serious offense and has to attend police station for clarification and as the matter of is of serious nature he or she has to be immediately attested digitally. Once the imposter come to know that the victim is in fear or accepted the narration then he or she is strictly directed not to contact anyone as he or she is under arrest and under investigation. The victim is asked to put their mobile phones for charging and open their camera and not to move outside view without permission.

Why people fall in trap

Fear: Fear of arrest and fear that if they don't cooperate further legal action would be taken.

Cyberspace novelties: As things are becoming digital, people presume that digital arrest is a new model of arrest.

Lack of awareness: Many individuals are not aware legal process and as the imposter create a real world look like environment by creating fake police station rooms, skype ID's, fake documents with seals etc to make individual believe in their narration.

Pressure tactics: Scammers isolate the victim and directs not to contact anyone hence the victim is unable to reach out anyone for help or advice. The scammers create of environment where the victim is pressured to act hastily hence the innocent individual falls into traps.

Conclusion

Digital arrest is inhuman form cybercrime. It deprives person's right to liberty and causes mental trauma and financial loss and hence the cybercriminal behind such offense should dealt with strict legal provisions. The efforts of Government of India is appreciable who have taken cybercrime seriously and taking all possible measures to curb the menace of cybercrime. Recently the honorable Prime Minister Modi has said that "agencies have blocked thousands of fraudulent video calling IDs, lakhs of SIM cards, mobile phones and bank accounts used for such scams." The Prime Minister has also addressed the gravity of issue of digital arrest and advised people to use a "stop, think and act" technique to counter such scams in case they receive such calls.

Digital arrest is illegal and sham. There has to be widespread awareness to tackle the menace of digital arrest. Digital arrest violates a person's fundamental right especially right to personal liberty and cause mental trauma and financial loss. A widespread campaign against cybercrime has to be launched through print and social media to create mass awareness. It would be suggested that the Government should release prerecorded messages in vernacular languages similar to which was launched during COVID period to create mass awareness about cybercrime especially digital arrest.