INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 2 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE DIGITAL HANDCUFFS: UNDERSTANDING DIGITAL ARRESTS

AUTHOR - SAHIL KIRAN GOKHALE, LAW ASPIRANT AT M.K.E.S. COLLEGE OF LAW

BEST CITATION - SAHIL KIRAN GOKHALE, THE DIGITAL HANDCUFFS: UNDERSTANDING DIGITAL ARRESTS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (2) OF 2025, PG. 65-68, APIS – 3920 – 0001 & ISSN - 2583-2344.

This article is published in the collaborated special issue of M.K.E.S. College of Law and the Institute of Legal Education (ILE), titled "Current Trends in Indian Legal Frameworks: A Special Edition" (ISBN: 978-81-968842-8-4).

INTRODUCTION:

What exactly does" cyber" mean? If you consult a traditional wordbook like Webster's, you'll find a description along the lines of " relating to or involving computers or computer networks. " That seems enough straightforward, right? When we suppose of cyber, we frequently imagine the image of a hacker in a hoodie, working down on their laptop, insulated in a dim room. It's easy to assume that cyber is each about technology. But is it really only about technology? That's the question worth exploring.

To understand cyber further completely, we need to look at its origins and literal environment. The term actually has roots in a field called cybernetics, which surfaced in the 1940s. Cybernetics concentrated on the proposition of communication and control, not just in machines but also in living organisms. It was n't simply about technology it was about the commerce between systems, both mechanical and natural.

Over time, the meaning of cyber has evolved. What sets cyber piecemeal from terms like IT security, computer security, or information security is its broader compass. Cyber is further than just guarding bias or data; it's about the complex relationship between technology, people, and associations. Yes, cyber is about technology, but it's also about much more. It represents a dynamic system where machines, humans, and institutions work together, shaping both openings and pitfalls. This is why we use the term " cyber " rather of limiting ourselves to terms like IT security or computer security — it encompasses a much broader, connected reality.Exploration and proposition suggest that it's veritably important to know what counts as Crime, not only for criminologists but also for anyone studying and trying to understand the cause of the detriment produced by crime. However, harms that might else be included are ignored, If the description of crime is too narrow. This was the case for times with domestic violence, ethnical hate, and much of what now counts as commercial and white- collar crime. Again, if the description is too broad, also nearly every divagation becomes a crime.

A farther consideration that makes defining crime important is that several policy opinions concerning social control are made grounded on a particular description of crime. These include the selection of precedence in policing and what to police, budget allocations for measures similar as crime forestalment programs, how to" handle" malefactors, and what a" crime-free" neighbourhood looks like.

In moment's connected world, the internet forms the backbone of ultramodern society,

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 2 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

easing communication, trade, and invention at an unequalled pace. still, as our reliance on digital structure grows, so does our exposure to a patient and frequently unnoticeable trouble cybercrime. currently as we all humans are getting close and use to mobile phones internet, social media as well as our fiscal deals which we do on our mobile phones are in once many times have fleetly taken a hike. [99]

Gone are the days when cybercrime was limited to the stereotypical image of a lone hacker; it has converted into a largely systematized and sophisticated assiduity, driven by motives ranging from fiscal gain to political manipulation and exploitation of advancing technologies. From ransomware attacks that cripple metropolises to phishing schemes targeting unknowing individualities, the compass of cybercrime is both expansive and intimidating.

What makes cybercrime particularly dangerous is its capability to transcend borders, painlessly targeting victims and associations across the globe. Critical means similar as particular data, intellectual property, and vital structure are decreasingly at threat, making cybercrime not only a matter of profitable concern but also a significant trouble to public security and particular sequestration. Its goods go beyond fiscal losses, eroding public trust in digital systems and raising critical questions about responsibility and data protection. As far as data protection is concerned we in India are at advanced pitfalls of getting attacked by a cybercriminal because still in this technosavy world there are still a lot of people who warrant the knowledge about how to cover their own particular data. his wide gap in understanding leaves people more susceptible to phishing swindles, identity theft, and unauthorized access to sensitive data.

As technology evolves, so too do the tools and tactics employed by cybercriminals, making it essential to borrow a forward- allowing and united approach to address these challenges. This composition delves into the complex world of cybercrime, examining its colourful instantiations, underpinning motorists, and the legal and technological strategies that can alleviate its impact. Addressing cybercrime is further than a specialized issue it is a global responsibility, demanding alert, collaboration, and invention at every position

Digital Arrest: Tools and Strategies to Counter Cybercrime :-

- ***Legislative Framework:***

The Indian Cyber Crime Coordination Centre issued a public advisory in reaction to the rising incidence of "digital arrest" crimes in India. Law enforcement agencies such as the CBI, police, customs, ED, or courts do not make arrests through video talks, the panel advised, cautioning the public against falling for these frauds[100]. It is illegal for law enforcement to make "arrests" using video calls or internet monitoring. If you receive such calls, it is clearly a scam. In reality, the recently enacted new criminal statutes prohibit law enforcement agencies from making a digital arrest. The law only allows the summons and procedures to be served electronically.

An instance was highlighted recently, it is also the longest digital detention case in India reported till now. In this case, a 77 year old lady from South Mumbai was targeted by fraudsters and kept under digital detention for more than a month. The accused duped her of 3.8 crore rupees and posed themselves as Mumbai Police officials. She first received a WhatsApp call where she was told that the parcel that she sent to Taiwan had been stopped which contained five passports, a bank card, 4KG clothes, MDMA drugs etc., to which she denied sending any parcel to anyone. Then she was told her Aadhar card details were used in crime. She was then asked to download Skype where Mumbai Police officials would interrogate her.

[99] https://egyankosh.ac.in/bitstream/123456789/59254/1/Kinds%20of%20Cyber%20Crime.pdf https://www.bbau.ac.in/dept/Law/TM/1.pdf

[100] https://lawchakra.in/blog/digital-arrest-scam-legal-protections-remedies/

There several fraudsters pretending themselves to be police officials ordered her not to cut the call, sought her bank account details and asked her to transfer money into the bank account given by them and also sent her a notice with a fake crime branch logo. They told her if they found money to be clear they would return it to her. She was also asked to continue the 24X7 video call with them.

Over some time she transferred 3.8 crore rupee to them, but when she didn't get back her money she suspected them and somehow managed to talk to her daughter about it and she asked her to approach to police. The police then freezed the accounts of fraudsters.

- ***Future Threats in Digital Arrest Scams:***

1. **Advanced Social Engineering:** Scammers are likely to employ more sophisticated techniques, such as deepfake technology, to create convincing impersonations of law enforcement officers, making it increasingly challenging for individuals to discern legitimate threats from fraudulent ones.

2. **Targeting Vulnerable Populations:** Elderly individuals and those less familiar with digital security are at heightened risk. Scammers may exploit these groups by tailoring their tactics to exploit their trust and lack of technological awareness.

3. **Integration with Other Cybercrimes:** Digital arrest scams may be combined with other forms of cybercrime, such as identity theft or financial fraud, leading to more complex and damaging attacks.

4. **Exploitation of Emerging Technologies:** The use of AI and machine learning could enable scammers to automate and scale their operations, making it easier to target a larger number of individuals with personalized scams.

- To safeguard against scams where individuals impersonate law enforcement officers, consider the following measures:

1. **Stay Informed:** Keep yourself and others updated on common scams and their warning signs. Recognizing these signs can help prevent falling victim to fraudulent schemes.

2. **Verify Identities:** If someone claims to be a law enforcement official, independently confirm their identity by contacting the relevant agency directly using official contact information found on their website. Avoid using contact details provided by the individual, as they may be fraudulent.

3. **Protect Personal Information:** Never share personal or financial details over the phone or internet unless you are certain of the recipient's legitimacy. Legitimate agencies will not request sensitive information through unsolicited communications.

4. **Report Suspicious Activity:** If you encounter a suspected scam, report it promptly to local authorities or appropriate organizations. Timely reporting can aid in investigations and help prevent others from becoming victims. By implementing these strategies, you[101] can enhance your protection against impersonation scams and contribute to broader efforts to combat fraudulent activities.[102]

Conclusion:-

In conclusion, as the digital ecosystem advances, the risks of cybercrime and digital arrests become more intricate and pervasive. The rise in scams that prey on people's trust, such as digital arrest frauds, highlights the need for increased awareness, better cybersecurity, and stronger regulatory frameworks. Since then, cybercrime has become a global problem that

[101] https://www.getcybersafe.gc.ca/en/blogs/protect-your-information-scams-impersonating-government- and-law-enforcement-agencies? https://www.interpol.int/en/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006- suspects

[102] https://www.google.com/url?sa=tCsource=webCrct=jCopi=89978449Curl=https://papers.ssrn.com/sol3/Delivery.cfm/5019885.pdf%3Fabstractid%3D5019885%26mirid%3D1Cved=2ahUKEwiGreaRypaLAxX1af UHHe-4CkEQFnoECA4QAQCusg=AOvVaw14DovQhb8OrCMdkBskLABg

affects individuals, companies, and nations equally.

To combat this growing threat, people need to be informed, take preventative measures, and verify their identities before acting. Businesses and governments must collaborate internationally, invest in technologies like encryption and artificial intelligence, and continuously enhance their cybersecurity plans in order to remain ahead of hackers. We can reduce the risks presented by digital threats and protect the integrity of our online interactions by cooperating and promoting a culture of awareness and education. To safeguard our digital future, the continuous combat against cybercrime calls on cooperation, flexibility, and creativity.[103]

Reference

1. YOGESH PRASAD KOLEKAR, CYBERCRIME IN INDIA: A GROWING THREAT TO CYBERSPACE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (2) OF 2025, PG. 47-49, APIS – 3920 – 0001 & ISSN - 2583-2344. Available Here - https://ijlr.iledu.in/cybercrime-in-india-a-growing-threat-to-cyberspace/
2. https://egyankosh.ac.in/bitstream/123456789/59254/1/Kinds%20of%20Cyber%20Crime.pdf https://www.bbau.ac.in/dept/Law/TM/1.pdf
3. https://lawchakra.in/blog/digital-arrest-scam-legal-protections-remedies/
4. https://www.getcybersafe.gc.ca/en/blogs/protect-your-information-scams-impersonating-government- and-law-enforcement-agencies?
5. https://www.interpol.int/en/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006- suspects
6. https://www.google.com/url?sa=tCsource=webCrct=jCopi=89978449Curl=https://papers.ssrn.com/sol3/Delivery.cfm/5019885.pdf%3Fabstractid%3D5019885%26mirid%3D1Cved=2ahUKEwiGreaRypaLAxX1af UHHe-4CkEQFnoECA4QAQCusg=AOvVaw14DovQhb8OrCMdkBskLABg
7. https://ijlmh.com/wp-content/uploads/Digital-Arrest-An-Emerging-Cybercrime-in-India.pdf

[103] https://ijlmh.com/wp-content/uploads/Digital-Arrest-An-Emerging-Cybercrime-in-India.pdf