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

CYBERCRIME IN INDIA: FINANCIAL FRAUD AND ITS GROWING THREAT TO THE ECONOMY

AUTHOR - RIDA FATEMA MOLEDINA, STUDENT AT M.K.E.S. COLLEGE OF LAW

BEST CITATION - RIDA FATEMA MOLEDINA, CYBERCRIME IN INDIA: FINANCIAL FRAUD AND ITS GROWING THREAT TO THE ECONOMY, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (2) OF 2025, PG. 86-89, 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).

ABSTRACT:

In an era dominated by *digital transactions, online transactions*, and the *ubiquity of technology,* the need for robust security measures has become paramount. The rise in *cyber-crime* has alarmed one and all, as the *cyber crooks* find innovative ways to fleece money by targeting gullible citizens from simple tricks like sending a 'link' to a victim's mobile to hack into their e-wallets, to intricate plots used to lure and snare people, especially those who are interested in investing in share market trading. Like many nations, India grapples with the challenges of securing its cyberspace and protecting sensitive data.

Keywords: Cybercrime, digital transactions, online transactions, ubiquity of technology, cyber criminals

Introduction:

Today we live in a technology driven world which is surrounded by automated smart technology, which has touched almost all spheres of human life, from military to medicine and from education to the election. We live in a world with boundaries which is secured but still it can be intruded virtually. This is real and this is cyberspace.[154]

Police commissioner Milind Bharambe said,[155]

"Cybercrime by share market trading scam has increased manifold. People need to be aware of investing in online share markets wherein they receive offers of high returns from unknown callers who initially give them returns to gain their trust. As the victim invests a huge amount, they are duped by the cyber crooks."

As technology advances and the internet becomes integral to daily life, cybercrime has emerged as a significant challenge that affects individuals, businesses, and government institutions alike.

The cybercrime statistics from the Navi Mumbai Police Commissionerate for the year 2023 indicate that 7,138 financial fraud cases were registered on the National Cyber Crime Reporting Portal (NCCRP), leading to a total loss of Rs. 67.55 crore for the victims. Moreover, 367 financial fraud cases were reported at different police stations, with the total amount defrauded reaching Rs. 80.47 crore.[156]

[154] https://www.geeksforgeeks.org/what-is-cyberspace/

[155] https://timesofindia.indiatimes.com/cyber-crimes-on-the-rise-in-navi-mumbai-as-fraudsters-find-multiple-ways-to-dupe-people/articleshow/112778753.cms

[156] Ibid

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 new boon brought by information technology has brought its scar in the form of cybercrime, moreover the new business environment required new regulations for its legal endorsement as more and more business communities are moving towards electronic commerce and transborder contracts. To address this issue the United Nation through its core agency United Nations Commission on International Trade Law (UNCITRAL)[157] had formulated model legislation on electronic commerce.[158]

Most common cyber-crimes[159]

Phishing: Cybercriminals deceive individuals by offering online part-time jobs, such as providing reviews for hotels or businesses. In exchange for completing these tasks, victims are promised monetary compensation. However, cybercriminals exploit this interaction to obtain personal information, including bank account details, leading to financial fraud. This is typically executed through fraudulent emails, websites, or messages that mimic legitimate sources but are designed to steal sensitive data.

Ponzi Scheme: Perpetrators attract individuals by promising exceptionally high returns on investments in stock market trading. Victims are encouraged to transfer money to various bank accounts, only to find that the promised returns never materialize, and the perpetrators fail to fulfill their commitments. This form of fraud often relies on deception and manipulation to entice individuals to invest.

E-Challan Fraud: Cybercriminals send counterfeit e-challan links, purporting to be from the traffic department to unsuspecting motorists. When the victim clicks the link to pay the traffic fines online, they are prompted to enter their details and are subsequently bombarded with multiple OTPs (One-Time Passwords). This leads to unauthorized debits from their bank accounts, with the cybercriminals making off with the funds.

Honey Trap: In this form of cybercrime, an individual, typically a male, is lured by a cybercriminal posing as a woman through social media or messaging platforms, such as WhatsApp. The fraudster befriends the target, gathers personal and confidential information, including sensitive bank account details, and ultimately exploits this data to carry out fraudulent transactions.

Sextortion: In this scheme, a cybercriminal, posing as a woman, initiates a video call with the victim, engages in inappropriate behavior, and coaxes the individual into participating in a similar act. The conversation is recorded, and the perpetrator later uses the footage to blackmail the victim, threatening to share the compromising video with the victim's family, friends, or colleagues unless a financial ransom is paid.

Ransomware Attacks: In these attacks, cybercriminals infiltrate a victim's computer or network, encrypting files and rendering them inaccessible. The attackers demand a ransom payment, often in cryptocurrency, in exchange for decrypting the files and restoring access. Failure to comply with the demands usually results in the permanent loss of the data or its public release.

Identity Theft: Cybercriminals steal personal information, such as Social Security numbers, addresses, and financial details, to impersonate individuals. This information is used to open fraudulent accounts, access financial resources, or commit other forms of fraud. Identity theft can have serious consequences for the victim, including financial loss and reputational damage.

Fake Tech Support Scams: Cybercriminals impersonate technical support agents from reputable companies, often claiming to detect malware or issues on a victim's computer. They

157 https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

158 Kolekar, Yogesh, A Review of Information Technology Act, 2000 (May 28, 2015). Available at SSRN: https://ssrn.com/abstract=2611827 or http://dx.doi.org/10.2139/ssrn.2611827

159 https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention

convince the victim to grant remote access to their devices or pay for unnecessary software or repairs. In some cases, sensitive information is stolen during the process.

SIM Swapping: In this fraud, cybercriminals trick mobile service providers into transferring the victim's phone number to a new SIM card that they control. Once successful, the criminals gain access to sensitive accounts, such as bank accounts or social media profiles, by receiving text-based authentication codes intended for the victim.

Deepfake Scams: Using AI-generated deepfake technology, cybercriminals create realistic yet fake videos or audio recordings of people to impersonate them. These fraudulent media are used to manipulate victims into making financial transfers, revealing sensitive information, or taking actions, they would not otherwise consider.

Cyberstalking: In this crime, perpetrators use digital platforms, such as social media, to stalk, harass, or intimidate their victims. Cyberstalking often involves repeatedly sending threatening or abusive messages, spreading false information, and attempting to create fear or distress for the targeted individual.

Malware Distribution: Malware, including viruses, worms, and trojans, is distributed via email attachments, infected websites, or compromised software. Once activated, the malware can steal data, damage files, and enable further exploitation of the victim's system for criminal purposes.

Impact of Cybercrime on the Indian Economy:

Cybercrime continues to have a profound impact on the global economy, with nations increasingly dependent on the Internet and digital technologies. Fraudsters exploit the anonymity provided by the Internet, along with computers and other digital devices, to facilitate illicit activities, often calculating that the potential monetary rewards outweigh the risks of being caught. The extent of cybercrime and its economic implications are critical for both governments and businesses, and understanding these effects is essential for developing updated legal, regulatory, and institutional frameworks.

To stay ahead in combating this emerging form of crime, courts and law enforcement agencies must be equipped with the necessary knowledge and tools. As the world economy becomes more interconnected and reliant on technology, the risks associated with cybercrime are becoming increasingly complex and multifaceted. The Indian economy is no exception to this growing threat. The impact of cybercrime both direct and indirect on India's economy is significant, influencing everything from unemployment rates to social services and foreign policy.

The severity of these effects has prompted many financial institutions, regulators, and governments worldwide to prioritize cybersecurity initiatives. According to the **World Economic Forum's 2023 Global Risks Report**, cyberattacks are ranked among the top global risks due to their potential to disrupt critical information infrastructure, enable illegal economic activities, and contribute to the breakdown of digital trust. The growing threat of cybercrime extends to cyber-laundering, which mirrors traditional money laundering. Cyber-laundering involves introducing illicit money into legitimate financial systems and then engaging in complex transactions to obscure the source of funds.[160]

The anonymity provided by the Internet, where individuals can disguise their location or use encryption technologies, has made cyber-laundering increasingly effective and difficult for law enforcement to detect. As cybercriminals operate with relative impunity, it is challenging for authorities to track and disrupt these illicit activities. In India, the economic cost of cybercrime is staggering estimated at **Rs 1.25 lakh crore** in 2019. As the Indian government continues to implement smart city projects and roll out nationwide network initiatives, the risks

[160] https://www.weforum.org/publications/global-risks-report-2023/digest/

posed by cyber threats are expected to rise, according to **Lt Gen (Dr) Rajesh Pant**, Coordinator of National Cyber Security.[161]

Conclusion:

The digital landscape is expanding rapidly. We are now storing more personal information online, including financial details and mobile numbers, than ever before, leading to an increase in cyber theft and the mishandling of sensitive data. With over 560 million internet users, India ranks as the second-largest online market, following China. This raises critical questions about the protection of our data and the adequacy of existing cyber laws.[162] Currently, aside from the IT regulations, India lacks comprehensive legislation addressing personal data protection.

The Government of India prioritizes cybersecurity low on its agenda, primarily due to significant resource constraints stemming from issues related to poverty and underdevelopment. It is reasonable to anticipate that awareness regarding cybersecurity among consumers, businesses, and policymakers will grow in the future. Although cultural shifts tend to be gradual, certain aspects related to cybersecurity, such as the tendency to share passwords, may evolve over time.

Most importantly, a balance between privacy[163] and security is essential in combating cybercrime, as the financial losses incurred from cyber fraud have detrimental effects on the economy. In light of the substantial challenges posed by these emerging cyber threats, both India and the global community must implement robust cybersecurity strategies to address the risks associated with cybercrime.

[161] https://www.business-standard.com/article/current-affairs/cybercrimes-caused-rs-1-25-trn-loss-in-2019-threats-will-spike-official-120102001373_1.html
[162] Kolekar, Yogesh, Protection of Data Under Information Technology Law in India (April 27, 2015). Available at SSRN: https://ssrn.com/abstract=2599493 or http://dx.doi.org/10.2139/ssrn.2599493
[163] https://blog.ipleaders.in/data-protection-laws-in-india-2/