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: A GROWING THREAT TO CYBERSPACE

AUTHOR - YOGESH PRASAD KOLEKAR, ASSISTANT PROFESSOR AT M.K.E.S COLLEGE OF LAW, MUMBAI, UNIVERSITY OF MUMBAI. EMAIL - PROFKOLEKAR@GMAIL.COM

BEST CITATION - YOGESH PRASAD KOLEKAR, CYBERCRIME IN INDIA: A GROWING THREAT TO CYBERSPACE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (2) OF 2025, PG. 47-29, 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

The evolution of Information and Communication Technology (ICT) has significantly transformed human society, impacting various aspects of life and altering the ways in which individuals learn, work, share, and engage in entertainment. Nevertheless, this evolution has also led to the emergence of a concerning phenomenon: the rapid increase in cybercrime. Cybercrime refers to illegal activities conducted through digital means, often targeting computer systems, networks, and online platforms. India's rapid digital adoption, fuelled by affordable internet access and smartphone penetration, has created a fertile ground for cybercriminals. Cybercrime is pervasive and disruptive, as demonstrated by both global and national statistics. Over 800 million Indians are internet users, attracting attention of cybercriminals. Initiatives like "Cyber Swachhta Kendra" promote cybersecurity hygiene among citizens, television ads, caution messages before calls are appreciative steps of the Government.

Keywords: cybercrime, ICT, online scams, Information Technology Act, 2000

Introduction

The advancement of technology and science has consistently been perceived as an indicator of human development and progress. Technological innovations are often viewed with optimism, as they are anticipated to introduce novel pathways for advancement. The evolution of Information and Communication Technology (ICT) has significantly transformed human society, impacting various aspects of life and altering the ways in which individuals learn, work, share, and engage in entertainment. Geographic distances and boundaries that once separated communities is virtually diminished by the emergence of the cyberspace. The proliferation of ICT has not only transformed communication methods but has also interconnected the global population within an extensive network, giving rise to a new domain known as the virtual world or cyberspace.[63]

In recent years, India has undergone a significant digital transformation characterized by notable advancements in technology and connectivity. Nevertheless, this evolution has also led to the emergence of a concerning phenomenon: the rapid increase in cybercrime. As India progresses towards a more interconnected and digitized society, cybercriminals are capitalizing on vulnerabilities, posing threats to individuals, businesses, and governmental institutions.

[63] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2611827

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

What is Cybercrime?

Cybercrime refers to illegal activities conducted through digital means, often targeting computer systems, networks, and online platforms. These crimes can take many forms, including hacking, phishing, identity theft, financial fraud, ransomware attacks, and cyberstalking. The motivations for engaging in cybercrimes encompass a variety of factors, including financial gain, espionage, personal hostility and acts of terrorism. The advent of internet technology has given rise to a new type of offenders known as cybercriminals, who exploit individuals' lack of technological knowledge and understanding of cyberspace. Consequently, cyberspace has become inundated with these criminals, who perceive significant opportunities for financial gain.

The term "cybercrime" is derived from the combination of "cyber" and "crime," denoting criminal activities conducted via the internet or within cyberspace. [64] It is noteworthy that the initial legislation pertaining to cyberspace, the Information Technology Act of 2000, primarily aimed to address issues related to e-commerce, e-governance, and electronic records, while largely neglecting the focus on cybercrime, as evidenced by its objectives and provisions. Cybercrime is pervasive and disruptive, as demonstrated by both global and national statistics. It is projected that the global financial impact of cybercrime will reach $10.5 trillion annually by the year 2025.[65]

The Rise of Cybercrime in India

India's rapid digital adoption, fuelled by affordable internet access and smartphone penetration, has created a fertile ground for cybercriminals. According to reports, India ranks among the top countries facing cyber threats. Key contributing factors include:

Increased Internet Usage: Over 800 million Indians are internet users, attracting attention of cybercriminals. Increased presence of users on internet also makes them exposed to cybercrime unless appropriate preventive measures are taken.[66]

Lack of Awareness: Many individuals and especially small businesses lack basic cybersecurity knowledge, making them vulnerable to cyber attacks like malware, digital arrest fake lottery scams etc. Individuals lacking cybercrime awareness may inadvertently disclose personal information, resulting in identity theft and fraudulent scams.

Rise in Digital Transactions: The widespread availability of smartphones, fast internet connections, and cutting-edge payment solutions has facilitated greater accessibility to digital transactions.[67]The growth of e-commerce and digital payment systems has attracted the interest of financial fraudsters, who perceive considerable opportunities for committing scams.

Common Forms of Cybercrime in India

Phishing Scams: Criminals pose as trustworthy organizations to obtain sensitive information, including passwords and credit card numbers. Phishing scams are a type of cyberattack where cybercriminal attempts to deceive individuals into revealing sensitive information, such as passwords, credit card numbers, or personal data.

Ransomware Attacks: Malicious software encrypts a victim's files, with perpetrators demanding a ransom for decryption. Ransomware attacks are a type of cybercrime in which malicious software (ransomware) encrypts a victim's files, rendering them inaccessible. The attacker then demands a ransom, usually in cryptocurrency, in exchange for the decryption key needed to restore access to the data.

[64] YOGESH PRASAD KOLEKAR, THE ROLE OF INDIAN CYBERCRIME COORDINATION CENTRE IN SAFEGUARDING CYBERSPACE, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (4) OF 2024, PG. 233-235, APIS – 3920 – 0001 & ISSN - 2583-2344.

[65] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[66] https://indianexpress.com/article/technology/tech-news-technology/indias-internet-users-to-surpass-900-million-in-2025-regional-content-driving-growth-iamai-kantar-report-9781881/

[67] https://pib.gov.in/PressReleasePage.aspx?PRID=2057013

Social Media Abuse: Issues such as cyberbullying, identity theft, and the creation of fraudulent profiles are widespread on social media platforms. This abuse can take many forms, ranging from targeted harassment to spreading misinformation, and its impact can be significant, affecting mental health, reputations, and even personal safety.

Financial Deception: Unauthorized transactions and fraudulent investment schemes are common where cybercriminal lures the victim to invest in fake investment schemes.

Government Initiatives and Legal Framework

The Indian government has taken several steps to combat cybercrime:

Information Technology (IT) Act, 2000: This legislation addresses cybercrimes and provides a legal framework for dealing with offenses like hacking, identity theft, and financial fraud. The Information Technology Act of 2000 is enforceable throughout India, including offenses that originate outside the country if they involve a computer, computer system, or computer network situated within India. With the implementation of the Information Technology Act, 2000, India has joined the select group of nations that possess distinct legislation to address issues related to information technology.[68]

Cyber Crime Cells: Specialized units have been established across states to investigate and resolve cybercrime cases. Cyber Crime Cells are police units that investigate cybercrimes. In India, citizens can file a complaint with a Cyber Crime Cell by calling the helpline number 1930 or using the National Cybercrime Reporting Portal.[69]

Awareness Campaigns: Initiatives like "Cyber Swachhta Kendra" promote cybersecurity hygiene among citizens, television ads, caution messages before calls are appreciative steps of the Government.[70]

CERT-In: The Indian Computer Emergency Response Team monitors and responds to cyber threats. CERT-In's main objective is to enhance security awareness and to offer technical support and guidance to assist in the recovery from cybersecurity incidents. CERT-In aims to actively contribute to the security of India's cyberspace and to establish a safe and reliable cyber ecosystem for its citizens. Its mission focuses on strengthening the security of India's communications and information infrastructure through proactive measures and effective collaboration.[71]

Conclusion

As India advances in its digital transformation, the challenge of cybercrime persists as a major concern. Addressing this issue necessitates a united approach that includes the government, private sector, and the general public. By promoting cybersecurity awareness and implementing cutting-edge technologies, India can reduce vulnerabilities and fully leverage the benefits of its digital evolution.

To protect oneself from the schemes of scammers, it is important to adopt precautionary steps, including the non-disclosure of financial information, avoiding the submission of banking details on unauthorized sites, and not installing remote access applications from unknown callers. Recent fraudulent activities, such as fake parcel scams and digital arrest scams, have caused considerable turmoil, leading to financial losses and emotional distress for many unsuspecting individuals. The government has made notable efforts by providing an online platform for reporting cybercrime. Enhancing awareness of cybercrime is a fundamental strategy in preventing these offenses.

[68] https://www.indiacode.nic.in/handle/123456789/1999
[69] https://cybercrime.gov.in/
[70] https://www.csk.gov.in/
[71] https://www.cert-in.org.in/