I J C R M

International Journal of Contemporary Research In Multidisciplinary

Review Article

Deep Dive in Pool of Cyberworld

Purvi Sharma*
Research Scholar, Department of Law, Sage University, Indore, Madhya Pradesh, India

Corresponding Author: *Purvi Sharma

DOI: https://doi.org/10.5281/zenodo.15132422

Abstract

The internet is the crux of life in the 21st century. Cyber security plays a vital role in the domain of information technology. Preservation of information from cyber frauds is a massive challenge that needs to be addressed effectively. Cybercrime is an activity that involves the transfer of information without user consent. This paper exemplifies numerous forms of cybercrimes, Laws framed out to counter cybercrime, and the role of the Indian judiciary. It also explains international laws and cybercrime's impact on society. Scope of study: The paper's main objective is to analyze the impact of cybercrimes on human rights, to focus on the national laws to prevent cybercrimes. This paper is descriptive and analytical, and the researcher has collected the data through a secondary method. The researcher has reviewed The Human Rights Communique, Volume II, Issue 1, published by the Newsletter for the Center for Advanced Studies in Human Rights, RGNUL, Punjab. This paper discusses human rights violations and cybercrimes, with a focus on social media and its role in advancing human rights. It provides a detailed examination of various treaties, highlighting the rights enshrined in them that are often infringed upon through cybercrimes. Additionally, the researcher referred to "Cyber Crime Scenario in India and Judicial Response" by Nidhi Arya, which explores cyberspace, defines cybercrimes, analyzes the implementation of cyber laws, and examines different forms of cybercrimes. Another significant reference is "A Critical Analysis on Judicial Activism about Cyber Law – An Indian Perspective" by V.M. Eshwar and Aswathy Rajan. This paper delves into various cybercrimes, their modes of commission, and the functioning of cyber laws in India.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 29-01-2025
- **Accepted:** 27-02-2025
- **Published:** 28-03-2025
- **IJCRM:**4(S2); 2025: 30-34

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Sharma P. Deep Dive in Pool of Cyberworld. Int J Contemp Res Multidiscip. 2025;4(S2):30-34.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Cybercrime, Cybersecurity, Information Technology Act, 2000, Human Rights Violations, Judicial Response to Cybercrime

INTRODUCTION

The widespread use of the internet across the globe has led to a significant rise in cyber fraud and crimes. In the 21st century, the digital space plays a crucial role in individuals' lives, shaping various aspects of society. However, the digital age functions as a double-edged sword—it offers numerous advantages while also posing substantial risks. Cybercrime has far-reaching consequences, impacting individuals, societies, nations, and the world at large. It encompasses a broad spectrum of criminal activities conducted through digital devices and networks. These crimes include fraud, identity theft, data breaches, computer viruses, online scams, and various other malicious activities facilitated by technology.

Various Forms of Cybercrimes

Virus Dissemination: These are malicious computer programs designed to infect systems or files and spread across networks. They disrupt computer operations and compromise stored data by either altering or deleting it.

Phishing: This involves stealing confidential information such as credit card details, usernames, and passwords by impersonating a legitimate organization. It is commonly executed through fraudulent emails (email spoofing) but can also occur via fake websites or phone calls.

Various Forms of Cybercrimes

Hacking: Hacking refers to the unauthorized access of another person's computer system.

Hackers are skilled programmers with an in-depth understanding of computer systems, often misusing their expertise for fraudulent purposes. They possess advanced proficiency in specific programming languages and dominate the internet space.

Identity Theft and Credit Card Fraud: Identity theft occurs when someone illegally acquires another person's identity to gain access to financial resources such as credit cards, bank accounts, or other benefits. Fraudsters may also use stolen identities to commit further crimes.

Software Piracy: Software piracy involves the unauthorized copying, distribution, or use of original software. This illegal practice undermines software creators by reducing their profits and discouraging investment in research and development. It also negatively impacts the global economy by redirecting funds from legitimate sectors.

Other Cybercrimes: Additional cyber offenses include internet fraud, cyberbullying, and child pornography, all of which pose significant threats to individuals and society.

Historical Background of Cybercrimes

Cybercrime first emerged in the 1870s, when teenagers were identified for engaging in telephone phreaking—manipulating telephone systems to make free calls. However, it was after the 1990s that cybercrime incidents increased significantly, gaining global recognition as a major threat to the economy and society.

In India, the first reported cybercrime case was Yahoo! Inc. v. Akash Arora (1999). The accused had unlawfully used the domain name "yahooindia.com," leading to a lawsuit where a permanent injunction was sought against him for trademark infringement.

Following this, India recognized that unauthorized access to another person's email account without their consent would be considered a cybercrime under Section 43 of the Information Technology (IT) Act, 2000.

In summary, the rise in technological advancements has directly contributed to an increase in reported cybercrimes worldwide.

Role of Indian Legislature in Combating Cybercrime

As society evolves, legal frameworks must adapt to emerging challenges. The increasing prevalence of cybercrime prompted the Parliament of India to enact stringent laws to counter digital threats. Consequently, the Information Technology (IT) Act, 2000 was introduced, accompanied by amendments to the Indian Penal Code (IPC), 1860, the Evidence Act, 1872, and the Banker's Book Evidence Act to align them with technological advancements.

Although the IT Act 2000 addresses cyber offenses and their corresponding punishments, it does not explicitly define cybercrime. The Act was primarily enacted to:

- Grant legal recognition to digital signatures and electronic records.
- Enable electronic bookkeeping for banks and other organizations.
- Protect online privacy and curb cybercrimes.

Amendments in 2008

The IT Act, 2000, was amended in 2008 to address:

Data privacy and security

- Regulation of digital signatures
- Corporate compliance for cybersecurity
- Countering cyber-enabled terrorism
- Preventing child pornography

The amended Act consists of 30 chapters and 90 sections, each addressing different aspects of cybersecurity:

- **Chapter II:** Digital and electronic signatures
- **Chapter III:** E-governance, electronic records, and digital signatures used by government agencies
- **Chapter IV:** Attribution, acknowledgment, and transmission of electronic records
- **Chapter IX:** (Section 43) – Civil penalties and compensation for damages caused by cybercrimes
- **Chapter XI:** (Sections 66A to 66F) – Criminal offenses related to cybercrimes

Key Sections of the IT Act, 2000 (Amended 2008)

- **Section 43:** Defines cyber offenses such as computer viruses, database theft, and unauthorized access. It is civil in nature and focuses on compensation for damages.
- **Section 66:** If an offense is committed with criminal intent, the offender faces criminal liability, including imprisonment, fines, or both.
- **Section 66A:** Sending offensive or misleading messages via electronic communication (email spoofing) can lead to imprisonment of up to 3 years and a fine. (This section was struck down by the Supreme Court in 2015 for violating free speech rights.)
- **Section 66B:** Dishonestly receiving a stolen computer resource or communication device can lead to 3 years of imprisonment or a fine of ₹1 lakh or both.
- **Section 66C:** Identity theft and misuse of electronic signatures or passwords can result in 3 years of imprisonment or a fine of ₹1 lakh or both.
- **Section 66D:** Cheating through impersonation via electronic means can lead to 3 years of imprisonment or a fine of ₹1 lakh or more.

- **Section 66E:** Violation of privacy, such as publishing private information without consent, is punishable by 3 years of imprisonment or a fine of ₹2 lakhs or both.
- **Section 66F:** Cyber terrorism—acts that threaten national security, disrupt critical systems, or spread computer contaminants leading to harm—carries a punishment of life imprisonment.
- **Section 67:** Publishing or transmitting obscene material, including child pornography, in electronic form is punishable under this section.

Cybercrime Provisions Under the Indian Penal Code (IPC)

The IPC also criminalizes cyber fraud and identity theft through the following provisions:

- **Section 464:** Making a false document or electronic record
- **Section 465:** Punishment for forgery
- **Section 468:** Forgery of an electronic record for cheating
- **Section 469:** Forgery of an electronic record to harm a person's reputation
- **Section 471:** Use of a forged document or electronic record.

Before the enactment of the Information Technology (IT) Act, the Evidence Act only recognized physical evidence in court. However, with the introduction of the IT Act, electronic documents and digital records are now legally admissible.

Crime is a significant challenge in society. While no society is entirely free from crime, its prevalence and severity—especially against women and teenagers—serve as indicators of societal well-being. Before the widespread adoption of the internet, crimes primarily occurred offline. However, as the internet became an essential part of daily life, it also facilitated the rise and proliferation of cybercrime.

Cybercrime impacts society in multiple ways

1. **Psychological Effects:** Victims, particularly women and teenagers, often experience stress, anxiety, and emotional distress due to cyber harassment, cyberbullying, or identity theft.
2. **Economic Consequences:** Cybercrime has global financial repercussions, leading to significant economic losses from fraud, data breaches, and online scams.

Women and teenagers remain the most vulnerable targets, underscoring the urgent need for stronger legal frameworks and awareness programs to combat digital crimes.

Role of the Judiciary in Cybercrime Cases

The judiciary plays a crucial role in addressing and resolving disputes arising from cybercrimes. Several landmark cases in India have shaped the legal framework for tackling cyber offenses.

Notable Cybercrime Cases in India

1. **Syed Asifuddin vs. State of Andhra Pradesh (2005)**
   This case, filed in the Andhra Pradesh High Court, dealt with mobile phone hacking and subscriber poaching.

Significance

- One of the first cases in India to address mobile phone hacking and its legal implications.
- Established the admissibility of computer source codes as evidence in cybercrime cases.
- Emphasized the responsibility of service providers to secure their networks and subscribers from unauthorized access.

2. **Avnish Bajaj vs. State (N.C.T. of Delhi) (2004)**
   Avnish Bajaj, the Managing Director of a classifieds website, was charged under Section 67 of the IT Act, 2000, for allegedly publishing obscene material.

Key Legal Issue

- Raised the distinction between an Internet Service Provider (ISP) and a Content Provider.
- Highlighted that the burden of responsibility falls on the content provider rather than the service provider.

3. **Bank NSP Case (State By Cyber Crime Police vs. Abubakar Siddique)**
   This case involved a management trainee at a bank who, along with his fiancée, misused the bank's computer systems. Following their separation, the woman created a fake email address under the name of the Indian Bar Association and sent fraudulent emails to the bank's foreign clients, leading to a loss of business.

Court's Ruling

- The bank was held liable for the fraudulent emails sent from its system.
- Reinforced the need for strong cybersecurity policies within financial institutions.

International Legal Frameworks on Cybercrime

While nations have enacted individual cybercrime laws, significant disparities in legal frameworks create jurisdictional challenges. Cybercriminals exploit these loopholes to operate across borders, making enforcement difficult. To address this, international treaties and conventions play a crucial role in harmonizing global cybersecurity laws.

Agreements like the Budapest Convention on Cybercrime and the United Nations resolutions on digital security help countries collaborate on cybercrime investigations, extradition, and data sharing. These frameworks promote standardized legal measures, ensuring that cybercriminals cannot escape justice due to inconsistent national laws.

By strengthening international cooperation, nations can enhance cyber threat intelligence sharing, improve incident response strategies, and build robust cybersecurity infrastructures. A unified global approach is essential to combat evolving cyber threats, protect digital assets, and ensure a secure cyberspace for all.

1. **Convention on the Rights of the Child (1989)**
- Adopted by the UN General Assembly (Resolution 44/25) on 20th November 1989, effective from 2nd September 1990.
- Article 34(c) mandates that state parties protect children from sexual exploitation, abuse, prostitution, and pornography.
- India ratified the convention on 11th December 1992, making it legally bound to comply with these protections.
- Article 3(1)(c) explicitly prohibits the production, distribution, and possession of child pornography, recognizing the internet as a medium for its dissemination.

2. **The Budapest Convention on Cybercrime (2001)**
Also known as the European Council Convention on Cybercrime, this treaty was adopted in 2001 and came into force in 2004.

Key Features
- Facilitates international cooperation between signatory nations.
- Mandates the criminalization of various cyber offenses, including hacking, identity theft, and cyber fraud.
- Includes a Protocol on Xenophobia and Racism in online spaces.

Despite calls for participation, India has not joined the Budapest Convention, citing concerns over sovereignty and lack of fair representation in its drafting process.

Impact of Cybercrimes on Human Rights
Cybersecurity plays a crucial role in safeguarding human rights by protecting privacy, personal data, and digital communications from cyber threats. However, cybercrimes violate several fundamental human rights enshrined in various international and national legal instruments.

Violation of Privacy Rights
The Universal Declaration of Human Rights (UDHR) - Article 12 and the International Covenant on Civil and Political Rights (ICCPR) - Article 17 state that:
"No one shall be subjected to arbitrary interference with their privacy. Everyone has the right to be protected by law against such interference."
In recognition of digital privacy, on December 18, 2013, the United Nations General Assembly passed a resolution emphasizing the right to privacy in the digital age.
In India, Article 21 of the Constitution, which guarantees the Right to Life and Personal Liberty, also extends to the right to privacy. Cybercrimes such as hacking, identity theft, data breaches, and unauthorized surveillance significantly infringe on this right.

Cybercrime's Impact on Other Human Rights

1. **Cyberbullying and Mental Health**
- Cyberbullying violates the right to the highest attainable standard of physical and mental health (Article 12 of the International Covenant on Economic, Social and Cultural Rights - ICESCR).
- Victims, particularly women and teenagers, suffer from psychological distress, anxiety, and depression due to online harassment and cyberstalking.

2. **Intellectual Property Violations**
- Cybercrimes such as hacking of trade secrets, copyright infringement, and intellectual property theft undermine the rights of innovators, businesses, and content creators.
- Intellectual property laws struggle to combat the rapid digital spread of pirated content and stolen innovations.

3. **Financial Security and Cyber Fraud**
- Credit card fraud, phishing scams, forgery, and identity theft cause financial distress to individuals and businesses.
- Many small businesses and startups suffer economic losses due to data breaches and cyber extortion.

Preventive Measures to Combat Cybercrimes
To mitigate the impact of cybercrimes, individuals and organizations must adopt strong cybersecurity practices, including:
- Using strong and regularly updated passwords.
- Enabling end-to-end encryption for sensitive communications.
- Avoid unknown or suspicious websites and links.
- Implementing intrusion detection systems in companies.
- Raising awareness about cyber threats and digital safety.

CONCLUSION
Cybercrimes have become a major threat to national security, economic stability, and individual privacy in the digital age. With the rise of advanced technologies, cybercriminals exploit vulnerabilities in networks, financial systems, and personal data, leading to fraud, data breaches, and cyber espionage. The widespread use of artificial intelligence (AI) has also enabled new forms of cyber threats, such as deepfake technology, which can be used for misinformation and identity theft.
Phishing scams, ransomware attacks, and financial frauds have significantly impacted businesses, governments, and individuals, causing billions in losses globally. Governments must implement strict cyber laws and continuously update their regulations to tackle emerging cyber threats. The Information Technology (IT) Act, 2000, along with global cybersecurity frameworks like the Budapest Convention, provides legal mechanisms to combat cybercrimes effectively. Digital rights protection is crucial in maintaining a safe online environment. Cybercriminal activities often violate fundamental human rights, including the right to privacy, security, and freedom of expression. International laws such as the General Data Protection Regulation (GDPR) and various UN resolutions, emphasize the importance of

safeguarding personal information and preventing digital exploitation. To mitigate cyber threats, organizations and individuals must adopt cybersecurity best practices, such as strong passwords, multi-factor authentication, encryption, and regular security audits. Additionally, public awareness programs and cybercrime reporting mechanisms can help prevent digital fraud. In conclusion, cybersecurity is a shared responsibility. Governments, businesses, and individuals must work together to enforce strict laws, strengthen digital infrastructure, and promote cybersecurity awareness. Ensuring robust legal frameworks and technological advancements will help create a secure cyberspace for all.

REFERENCES

1. Anisha. Awareness and strategy to prevent cybercrimes—Indian perspective. *Indian Journal of Applied Research* [Internet]. Vol. VII; Available from: https://www.worldwidejournals.com/indian-journal-of-applied-research-(IJAR)/article/awareness-and-strategy-to-prevent-cybercrimes-an-indian-perspective/MTE3NDc=/?is=1
2. Sunita. Cybercrimes and laws. *METRAIL* [Internet]. 2020. Available from: http://dcac.du.ac.in/documents/E-Resource/2020/Metrail/408sunitayadav4.pdf
3. IBF (Indian Bankers Forum). Cyber laws in legal perspective. *Cyber Laws Chapter in Legal Aspects Book* [Internet]. Available from: https://ibf.org.in/documents/cyber-laws-chapter-in-legal-aspects-book.pdf
4. United Nations Office on Drugs and Crime (UNODC). About UNODC [Internet]. Available from: https://www.unodc.org/unodc/en/about-undoc/index.html
5. Prasad A. Cybercrime in India—Time series study of state-level data. *ResearchGate* [Internet]. 2020. Available from: https://www.researchgate.net/publication/342509526_Cyber_Crime_in_India_Time_Series_Study_of_State_Level_data.

About the Corresponding Author

Purvi Sharma is a Research Scholar at Sage University, Indore, specializing in cyber law and human rights. Her research explores cybercrime, legal frameworks, and judicial responses, focusing on the evolving challenges of law in the digital era.