MULTIDISCIPLINARY COSMOPOLITAN JOURNAL OF RESEARCH
(MUCOJOR)-2583-9829(Online)
International Peer Reviewed and Referred E-Journal
ISSN: 2583-9829, Volume: 02, Issue: 04, December 2024

Cybercrime: Understanding Basic Legal Definitions and Offences

Dr. Lata Indubhai Mulchandani

Assistant Professor

Shri Dhanjibhai D Kotiyawala Municipal Law College, Porbandar

Abstract

Cybercrime largely involves the misuse of the computer and the internet to obtain private information about a person, either indirectly or directly and then to illegally or without the person's knowledge reveal it on online platforms with the intention of tarnishing the person's reputation or causing them harm, either. Cybercrime encompasses a wide range of criminal activities that are carried out using digital devices and/or networks. These crimes involve the use of technology to commit fraud, identity theft, data breaches, computer viruses, scams, and expanded upon in other malicious acts.

Key words: Cybercrime, Fraud, Hacking, criminal offences, digital technologies

Introduction:

Cybercrime refers to criminal activities committed using computers, internet, or other digital technologies, harming individuals, organizations, or society. Crimes committed using computers, internet, or other digital technologies. “Cybercrime" includes unauthorized access, hacking, data theft, spreading malware, identity theft.

Review OF Literature

A literature review on **cybercrime and offences** involves examining various studies, reports, and theoretical discussions that provide insight into the nature, extent, types, and impact of cybercrime. It also explores the legal frameworks, enforcement challenges, and evolving trends in cyber-related criminal activities. Below is a structured review:

MULTIDISCIPLINARY COSMOPOLITAN JOURNAL OF RESEARCH
(MUCOJOR)-2583-9829(Online)
International Peer Reviewed and Referred E-Journal
ISSN: 2583-9829, Volume: 02, Issue: 04, December 2024

Cybercrime: Understanding Basic Legal Definitions

- **International Definitions**:

1. United Nations (UN): "Cybercrime refers to any criminal activity committed using computers, computer networks, or other digital technologies."

2. Council of Europe (COE): "Cybercrime is a criminal offence committed using electronic communication networks or information systems."

3. Interpol: "Cybercrime is any crime committed using computers, computer networks, or other digital technologies."

- **National Definitions (India)**

1. Information Technology (IT) Act, 2000: "Cybercrime includes unauthorized access, hacking, data theft, spreading malware, identity theft."

2. Indian Penal Code (IPC), 1860: "Cybercrime includes online fraud, identity theft, cyber stalking."

- **Academic Definitions**:

1. Oxford Dictionary: "Cybercrime is criminal activity involving the use of computers or the internet."

2. Merriam-Webster: "Cybercrime is criminal activity related to or involving computers or computer networks."

- **Organizational Definitions**:

1. FBI (Federal Bureau of Investigation): "Cybercrime is any crime committed using computers, computer networks, or other digital technologies."

2. CERT-In (Indian Computer Emergency Response Team): "Cybercrime includes unauthorized access, hacking, malware, phishing.

MULTIDISCIPLINARY COSMOPOLITAN JOURNAL OF RESEARCH
(MUCOJOR)-2583-9829(Online)
International Peer Reviewed and Referred E-Journal
ISSN: 2583-9829, Volume: 02, Issue: 04, December 2024

❖ **Cybercrime: Various Types of Offences:**

Computer-related offences	**Content-related offences**	**Conduct-related offences**	**Specific offences**	**Cyber terrorism (threatening national security)**
1.Hacking (unauthorized access) 2. Malware attacks (viruses, trojans) 3.Data theft/breaches 4.Network disruption (DDoS) 5.Computer vandalism (damage/destruction)	1.Child pornography 2. Online harassment/stalking 3. Defamation/slander 4.Copyright infringement 5. Obscene material distribution	1. online fraud (phishing, scams) 2. Identity theft 3.Cyber terrorism 4.Online gambling 5.Human trafficking	1. spamming 2. Phishing 3 Ransomware attacks 4.SQL injection 5.Cross-site scripting (XSS)	Cyber warfare (state-sponsored cyber-attacks)

❖ **Computer related offences:**

➢ **1.Hacking (Unauthorized Access)**

Hacking refers to unauthorized access, disruption, or damage to computer systems, networks, or electronic data.

➢ Types of Hacking: 1. Black Hat Hacking (malicious) 2. White Hat Hacking (ethical) 3. Grey Hat Hacking (combination of black and white)

➢ Hacking Techniques: 1. Phishing 2. SQL Injection 3. Cross-Site Scripting (XSS) 4. Malware 5. Cross-Site Request Forgery (CSRF) 6. Brute Force Attacks 7. Social Engineering

➢ **2. Malware Attacks (Viruses, Trojans)**

Malware (malicious software) is harmful software designed to disrupt, damage, or unauthorized access to computer systems or data.

➢ Types of Malwares:

1. Viruses: Replicating malware, attaching to files/programs.

2. Trojans: Disguised malware, allowing unauthorized access.

3. Worms: Self-replicating malware, spreading through networks.

4. Spyware: Monitoring user activity, stealing sensitive info.

5. Adware: Displaying unwanted ads.

6. Ransomware: Encrypting data, demanding payment.

7. Rootkits: Hiding malware from system detection.

- **3.-Data Theft/Breaches**

Unauthorized access, disclosure, or theft of sensitive information, compromising confidentiality, integrity, or availability.

- Types of Data Breaches: 1. Hacking/Unauthorized Access 2. Insider Threats 3. Physical Theft/Loss 4. Accidental Exposure 5. Social Engineering

- **4- Network Disruption (DDoS)**

Distributed Denial-of-Service (DDoS) attack, flooding a network/resource with traffic to disrupt or render it unavailable.

- Types of DDoS Attacks: 1. Volumetric Attacks (bandwidth exhaustion) 2. Application Layer Attacks (targeting specific apps) 3. Protocol Attacks (exploiting network protocols) 4. Amplification Attacks (using third-party services)

- **5.Computer Vandalism (Damage/Destruction)**

Intentional damage or destruction of computer systems, networks, or electronic data.

- Types of Computer Vandalism:

1. Data destruction 2. System crashes 3. Network disruption 4. Hardware damage 5. Software sabota

- **Content-related offences:**

1.Child Pornography

Creating, distributing, or possessing images or videos depicting minors in sexually explicit situations.

MULTIDISCIPLINARY COSMOPOLITAN JOURNAL OF RESEARCH
(MUCOJOR)-2583-9829(Online)
International Peer Reviewed and Referred E-Journal
ISSN: 2583-9829, Volume: 02, Issue: 04, December 2024

2.Online Harassment/Stalking

Repeated, unwanted online behaviour intended to intimidate, threaten, or harm.

3.Defamation/Slander

Spreading false information to harm someone's reputation.

4. Copyright Infringement

Unauthorized use or distribution of copyrighted material.

5.Obscene Material Distribution

Distributing content deemed obscene or harmful.

❖ **Conduct-related offenses:**

1.Online Fraud (Phishing, Scams)

Deceptive online activities to steal sensitive info or money.

➢ Types: ‣ Phishing‣ Email scams‣ Social engineering ‣ Fake websites ‣ Online auction scams

2.Identity Theft

Stealing personal info to impersonate or commit crimes.

➢ Types: ‣ Credit card theft‣ Social Security number theft‣ Password theft

3. Cyber Terrorism

"Using technology to disrupt or harm critical infrastructure.

➢ Types: ‣ Hacking‣ Malware attacks‣ DDoS attacks

4. Online Gambling

Participating in unauthorized online gaming activities.

➢ Types: ‣ Sports betting‣ Casino games‣ Poker

5. Human Trafficking

Exploiting individuals for labour or commercial sex.

- Types: ‣ Sex trafficking‣ Labor trafficking

❖ **Specific offences:**

1. Spamming

Unsolicited commercial emails, messages, or comments.

- Types: ‣ Email spam‣ Comment spam‣ Messaging spam

2. Phishing

Deceptive emails/messages to steal sensitive info.

- Types: ‣ Email phishing‣ SMS phishing (smishing)‣ Social media phishing

3. Ransomware Attacks

Malware encrypting data, demanding payment.

- Types: ‣ Crypto-ransomware‣ Lockscreen ransomware

4.SQL Injection

Malicious SQL code injection to access databases.

- Types: ‣ Classic SQL injection‣ Blind SQL injection

4. Cross-Site Scripting (XSS)

Injecting malicious scripts into websites.

- Types: ‣ Stored XSS‣ Reflected XSS‣ DOM-based XSS

❖ **Cyber terrorism (threatening national security)**

- Cyber terrorism is a threat to national security that involves the use of disruptive activities or threats against computers and networks. Cyber terrorists can cause chaos, disrupt critical infrastructure, and threaten national security. Some of the methods they use include:
- Advanced persistent threat (APT) attacks

These sophisticated attacks use concentrated penetration methods to gain network access. APT attackers can stay undetected in a network for a time to steal data.

❖ **State-sponsored cyber attacks**

(SSAs) are cyber-attacks carried out by a government against another country's government or organization. They can cause long-term damage to a target's business or government.

❖ **Challenges in Cybercrime Investigation and Prosecution**

- **Jurisdictional Issues**: Cybercrime often transcends borders, making it challenging to investigate and prosecute when perpetrators reside in different countries. International cooperation is required, but differences in legal frameworks create barriers.
- **Attribution Difficulties**: Identifying and attributing cyber-attacks to specific individuals or groups is a technical challenge. Criminals use anonymization techniques like VPNs and the dark web to mask their identities.
- **Lack of Expertise and Resources**: Law enforcement agencies often lack the technical expertise and resources needed to combat cybercrime. This is particularly problematic for smaller nations and organizations.
- **Legal Frameworks**: Many legal systems have not fully adapted to the unique characteristics of cybercrime, and laws are often outdated. Some nations have developed specific cybercrime laws, such as the Computer Fraud and Abuse Act (CFAA) in the U.S., but gaps remain globally.

❖ Conclusion

Cybercrime is a broad range of criminal activities that use digital devices and networks to commit fraud, identity theft, and other malicious acts. Cybercrime can have serious consequences for individuals, businesses, and governments, and there are many ways to combat it.

Certificate No.:020412202404

MULTIDISCIPLINARY COSMOPOLITAN JOURNAL OF RESEARCH

(MUCOJOR)-2583-9829 (On-line)

International Peer Reviewed and Refereed Journal

Certification of Publication

The Board of Multidisciplinary Cosmopolitan Journal of Research (MUCOJOR) is hereby awarding this certificate to

Dr. Lata Indubhai Mulchandani

In recognition of the publication of the paper entitled

Cybercrime: Understanding Basic Legal Definitions and Offences

Published in Volume 02, Issue 04, December 2024.

EDITOR IN CHIEF