SCENARIO OF MODERN CYBERCRIMES AND CYBER LAWS IN INDIA

Divyani Newar, National Education Foundation (NEF) Law College, Guwahati, Assam

ABSTRACT

Cybercrime is a relatively new concept. It began to gain importance with the development of technology and increase in internet users worldwide. The Internet is not confined to any territory; it is borderless and spread across nations due to its accessibility. It is considered a boon as it has made life easy for humans, but on the other side, cybercrime acts as the bane in this boon. It is a unique type of crime that takes place in the virtual space, perpetrated by individuals whose identities are hidden. The criminals can execute their acts from miles away, using technology without any physical contact with their victims. Cybercrimes are committed for various reasons, such as causing harm to the victim's reputation, emotional well-being, mental health, and financial stability among other reasons. It can affect any section of society, whether it is private individuals, large-scale private or governmental organizations, or even children who are not spared from such acts. India is one of the most vulnerable countries in the world, suffering heavy losses due to increasing incidents of cybercrime each year. The legislature has enacted several laws to address these issues, including the IT Act of 2000, the new criminal laws of 2023 (which replaced the old criminal laws), and the DPDP Act of 2023. This paper aims to highlight the growing issue of cybercrime, its various categories, the profound impact it has on society, and the enforcement of laws to combat these issues in the country.

Keywords: Internet, Cybercrime, Cyberlaws, Legislature, Technology

INTRODUCTION

In this digital era, the internet, a modern network of communication over which millions of computers are connected, has become an integral part of every aspect of life. The transmission of data and information across different networks has been facilitated by the adoption and utilization of the internet, also known as cyberspace, which has enhanced the efficiency of such communication.[1] It has made daily tasks such as business transactions, online banking, internet shopping, booking tickets online, and e-learning more convenient.

Internet usage skyrocketed, particularly in the wake of the recent pandemic, which ushered in a new era of digitisation across all sectors be it business, education, and government. The heavy reliance on computers and the internet has resulted in a rise in online crimes, known as cybercrime, which is a relatively new concept. Cybercrime refers to any crime committed over the internet or related technologies that have the potential to impact everyone, from private individuals to large-scale organisations and cause a considerable amount of damages. Cybercrimes are committed for various reasons, including causing reputational, emotional, mental agony, and financial loss to the victims. According to recent reports, there were over 740,000 complaints filed on the National Cybercrime Reporting Portal (NCRP) under the Ministry of Home Affairs. This resulted in Indians losing more than Rs 1,750 crores to cybercrime between January and April 2024.[2]

There are different categories of cybercrimes, each based on different incidents that create controversy, leading to the use of various terminologies. The Indian Cybercrime Coordination Centre (ICCC) has classified cybercrimes into 8 main categories.

Very few laws are in place to protect cybersecurity in India. The first ever legislation passed in India to deal with cybercrime related issues was the Information Technology Act, 2000 based on the United Nations Commissions on International trade Law (UNCITRAL) model. In order to safeguard and protect the data and privacy of individuals and organizations amidst advancing technology the Digital Personal Data Protection (DPDP) Act of 2023 was introduced by the Parliament of India which is yet to be implemented. The new criminal laws that replaced the

[1] Divakar Sharma. *A Study on Cyber Crime and its Related Laws in India*, 20 JES 1080, 1080-1081 (2024).
[2] *Here is how much Indians lost to cyber frauds between Jan and Apr of 2024*, BUSINESS STANDARD, (Aug 24, 2024, 09:07 PM), https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html.

old ones have highlighted the complexities of the digital age and include provisions for offenses committed in the internet era.

This paper aims to briefly discuss the issue of cybercrime, its various categories, and its profound impact on society. It also delves into the current major laws enforced in India, among other laws, to combat these issues.

CONCEPT OF CYBERCRIME AND ITS CATEGORIES

The Oxford dictionary defines Cybercrime as crime which is performed by means of the internet.[3] Any crime committed over the computer network or the internet or as recognised by the Information Technology Act, 2000 maybe called a cybercrime or electronic crime (e-crime).[4] It is a result of the rapid advancements in the domain of information and communication technology (ICT) and refers to a broad range of criminal activities conducted over the computer and computer networks ranging from electronic cracking to cyber-attacks such as denial-of-service (DoS) attack and can also refer to traditional offences made possible with the use of the same.[5] There is however no standard definition of the term and mainly restricted to individual understanding.

Cybercrimes can be committed against a private individual, a group of individuals and large-scale private or public organisations. These crimes are committed for different reasons such as to extort money from individuals, to blackmail or cause mental agony by harassing the victim for whatever reasons, steal or destroy the personal information of individuals or secret data of organizations and information warfare among other activities which may pose a threat to the financial stability and security of any nation. It also covers areas of law which include the right to privacy, freedom of expression and intellectual property rights such as copyright, patent and trademark and crimes even committed outside the jurisdiction of India.[6]

One classification is given by Gordon and Ford who classify cybercrime into two categories using a continuous scale: Type I and Type II. Type I includes technical offenses such as hacking, while Type II involves more human interaction, such as online gambling. Nevertheless, the

[3] *Definition of Cybercrime noun from the Oxford Advanced Learner's Dictionary*, (Aug 15, 2024, 06:54 PM), https://www.oxfordlearnersdictionaries.com/definition/english/cybercrime.
[4] Jatin Patil, *Cyber Laws in India: An Overview*, 4 IJLLR 1, 2-3 (2022).
[5] Osman Goni, *Cyber Crime and Its Classification*, 10 IJEEA 1, 1-2 (2022)
[6] Manjeet Singh et al, *A Comprehensive Study of Cyber Law and Cyber Crimes*, 3 IJIEASR 20, 20-21 (2014).

authors claim that there are extremely few instances that are likely to be categorised as Type I or Type II and mark the end to a continuum. The emergence of artificial intelligence and advancements in the field of robotics are swiftly making changes to the scene of technology which in turn could be capable of giving rise to a third scene i.e., Type III influenced by the act of self-learning.[7]

A modern example of cybercrime is the conduct of a hacktivist who is a person who undertake protests against the activities and policies of an organization. The most notable incident was the attack by the anonymous hacktivist in the year 2010 on giant organisations such as the Mastercard, PayPal and Visa as a revenge for their decision to cease taking donations to the WikiLeaks group.[8]Another type of attack is the Distributed Denial of Service (DDoS) where there is an attempt to make inaccessible an online service by flooding it with traffic from several sources causing it to crash. For the organization PayPal the impact was alone estimated to be USD 5.5 million. With the aid of resources that are readily available online, cybercrimes can be committed easily and affordably. However, the primary concern for the government is that cybercriminals from any part of the world can use the internet to conduct espionage and spread terrorism.[9]

As per the Ministry of Electronics and Information Technology, the reported incidents of phishing were more than double the number by the year 2021. Data recovered under the Department of Cybercrime, Government of India highlighted the fact that by the year 2022 there were more than 61,000 cases of fraud committed under digital payments section. [10] The Indian Cybercrime Coordination Centre (ICCC) has categorised Cybercrimes under 8 main categories. They are Child Sexual Abuse Material, Cryptocurrency Crime, Cyber Terrorism, Damage to Computer Systems, Online Financial Fraud, Online and Social Media Related Crime, Publishing Explicit Material in Electronic Form and Ransomware.

i. **Child Sexual Abuse Material:** Also known as child pornography is any content which contains sexual images of a child in any manner or who has been exploited sexually. It is illegal and punishable under section 67B of the Information Technology Act, 2000.

[7] Rick Sarre et al, *Responding to cybercrime: current trends*, 19 PPR 515, 515-516 (2018).
[8] Ibid.
[9] Ibid.
[10] Tanya Gupta, *Emerging Trends of Cybercrime in India: A Contemporary Review*, 8 JLPT 57, 57-58 (2023).

ii. **Cryptocurrency Crime:** Under this category, three types of crimes are categorised:

   a. Cryptojacking, which occurs when a perpetrator stealthily exploits a victim's computing power to generate cryptocurrency.

   b. Cloud Mining and Crypto Mining Scams, which involve malware that extracts or steals resources from infected machines, having a significant negative impact in their performance and,

   c. Investment Frauds related to Cryptocurrency is an opportunity to fraudulently make investments in cryptocurrency with promised high returns.

iii. **Cyber Terrorism:** An act is carried out to endanger the integrity, sovereignty or unity of a nation and incite fear among its population by extracting sensitive information from computer systems restricted for reasons of national security.

iv. **Damage to Computer Systems:** Also known as Hacking is the act of gaining illegal access to a user's account.

v. **Online Financial Fraud:** An act by cybercriminals to make monetary gains with the help of computer system.

vi. **Online and social media Related Crime:** The act of using social media to cause harm to individuals in any form, be it reputational, emotional, mental, or financial. Some examples include email phishing, cyberstalking, sexting, and online job or matrimonial fraud, among many others.

vii. **Publishing Explicit Material in Electronic Form:** Publishing of content containing sexually explicit acts via electronic medium for the purpose of corrupting individuals is a punishable crime under the IT Act, 2000.

viii. **Ransomware:** It involves cybercriminals demanding a ransom in exchange for restoring encrypted data of victims which can include individuals as well as organizations.[11]

[11] *Cybercrime Categories*, INDIAN CYBERCRIME COORDINATION CENTRE (Aug 24, 2024, 10:00 PM) https://i4c.mha.gov.in/cyber-crime-categories.aspx.

LAWS TO PROTECT CYBERCRIMES

Information Technology Act, 2000

Based on the dependency of society on the virtual or digital space, there was a need to regulate it. Thus, the legislature enacted the Information Technology Act, 2000 based on the United Nations Commission on International Trade Law (UNCITRAL) model which placed a strong emphasis on giving legal recognition to electronic records and transactions taking place online. Later amendments were made to the act in the year 2008, giving rise to the Information Technology Act, 2008.

The Information Technology (IT) Act, 2000 is the sole codified law relating to digitisation in India which has only undergone one major change in the year 2008.[12] The IT Act, 2000 was passed by the Indian government in order to address concerns about the legal acceptance of electronic documents, the electronic filing of documents with government departments, digital signatures, violations, offences, and the Justice Dispensation System of cybercrimes. The Indian Evidence Act of 1872, the Indian Penal Code of 1860, the Bankers' Book Evidence Act of 1891, the Reserve Bank of India Act of 1934 were also amended by it.

The Information Technology Amendment Act, 2008 focuses on issues such as data privacy, information security, making neutral digital signatures, defining cybercafé, outlining appropriate security practices that corporates need to follow, redefining the role played by intermediaries, acknowledgement of the role and function of the Indian Computer Emergency Response Team (CERT-In), inclusion of cybercrimes such as child pornography, cyberterrorism and authorization of Inspector to inspect the cyber-related offences as opposed to the Deputy Superintendent of Police (DSP) earlier.[13]

Digital Personal Data Protection Act, 2023

In today's world, data privacy is crucial. Organizations collect a significant amount of information about individuals, both online through social networking, dating, and matrimonial websites and offline through hospitals, banks, and shopping complexes among others. This collected information often reveals a lot about a person's personality and can be classified as

[12] Ivneet Kaur Walia & Dinesh Kumar, *Need for Revamping Information Technology Laws in India*, 8 JLS 202, 203-204 (2021).
[13] Shailesh P. Thakare et al, *A Review on Information Technology and Cyber Laws*, 2 IJEAS 10, 12-13 (2015).

private information. A majority of nations have shed light on data privacy as an integral part of the right to privacy leading them to frame laws to protect the data of individuals as a part of that right.[14] The Digital Personal Data Protection (DPDP) Act, 2023 was introduced under the act of Parliament of India with the aim to safeguard and protect data and privacy of individuals and organizations amidst the growing technological advancements. The DPDP Act aims to achieve a greater level of accountability and responsibility for organizations functioning under the jurisdiction of Indian law. The official notification for the enactment of the act is yet to come into effect.[15] This is the first law of its kind in the country, aimed at safeguarding the personal data of citizens. It draws inspiration from Europe's General Data Protection Regulation (GDPR) and consists of nine chapters and one schedule.[16]

The Three New Criminal Laws

To make changes to the existing criminal laws from the colonial era, such as the Indian Penal Code of 1860, the Code of Criminal Procedure of 1973 and the Indian Evidence Act of 1872, the Indian Parliament enacted the three new criminal bills. These bills are the Bharatiya Nyaya Sanhita, 2023 (BNS) which replaced the Indian Penal Code, 1860 (IPC), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) which replaced the Code of Criminal Procedure, 1973 (CrPC) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) which replaced the Indian Evidence Act, 1872 (IEA).

These new laws came into effect on July 1st, 2024 and include a number of new provisions tailored to the needs of modern society and emerging technologies.[17] The previous criminal laws will continue to hold significance unless all pending cases related to it are disposed of. The new criminal laws have shed light into the intricacies of the digital age and makes provisions to tackle crimes committed in the internet era.

A significant addition has been made in the new criminal laws under the section of ‘organised crime’ and defines it as any criminal activity such as cybercrimes and offenses of economic

[14] Radha Ranjan, *Right to Privacy*, 4 IJLRG 87, 94-95 (2018).
[15] Pradip Kashyap, *Digital Personal Data Protection Act, 2023: A new light into the Data Protection and Privacy Law in India*, 2 ICREPJIS 1, 1-2 (2023).
[16] Chanlang Ki Bareh, *Reviewing the Privacy Implications of India's Digital Personal Data Protection Act (2023) from Library Contexts*, 44 JLIT 50, 51-52 (2024).
[17] ET Online, *New criminal laws enacted from today: All you need to know about them*, THE ECONOMIC TIMES (Aug. 22, 2024, 11:00 PM), https://economictimes.indiatimes.com/news/how-to/new-criminal-laws-enacted-from-today-all-you-need-to-know-about-them/articleshow/111391637.cms?from=mdr.

nature performed by any single individual or a group of individuals together acting on behalf of a crime syndicate. Hence, the BNS incorporates provisions to tackle cybercriminals which was not addressed under IPC.

The BNSS has introduced the provisions of audio or video mode of communications and electronic communications under the section of digital technologies in order to reduce the duration of criminal proceedings in court procedures. As per the provisions of BNSS, the accused and witnesses can now receive summons via electronic means of communication. Investigating officers can use audio-visual technology to record statements, search and seizure operations, and other legal proceedings such as appeals and trials, which can be conducted electronically. This is intended to expedite the enforcement procedure against all crimes, including cybercrimes.

Section 57 of the BSA acknowledges electronic records, such as digital documents, emails, social media posts, among many others as primary sources of evidence in court proceedings. This marks a significant change from previous laws that considered such evidence as secondary. This recognition saves the Court's valuable time by granting electronic records the status of primary evidence, as opposed to previous physical copies of digital evidence.[18]

CONCLUSION

In today's technologically advanced era, there is a growing dependence on the internet, leading to a rise in crimes committed in cyberspace, known as cybercrime. It is a result of rapid advancement in information and communication technology. This kind of crime is borderless and spreads across every country, affecting every level of society. It ranges from children falling victim to offenses such as child pornography linked to sexual abuse to nations being targeted by cyberterrorism. Every year India witnesses huge financial losses due to online frauds which also needs to be addressed. The Indian legislature consistently strives to keep pace with technological advancements by amending existing laws and incorporating provisions that address the current needs of society, particularly in the digital age. This is one of the reasons for the enactment of the three new criminal laws which replaces the old laws.

[18] Sajai Singh et al, *Stringent measures against cybercrimes in India's new criminal justice system*, JSA ADVOCATES AND SOLICITORS (Aug. 22, 2024, 11:00 PM), https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system/.

However, the current laws in our country may be unable to keep up with the rapid development of technology. It's important to remember that while the system may have its flaws, users also have a responsibility to follow the protocols set out by authorities when using internet-related services. The issue needs to be addressed by collaborating with other countries on the international front, implementing stricter laws and punishments for violators, and raising awareness. A significant portion of the population is still uninformed about this increasing threat. These steps are crucial in combating the escalating problem, which is currently lacking in today's cyber laws.