

A Discussion on Cybercrimes with Reference to the Information Technology Act, 2000

Indrayudh Chowdhury*, Nimish Sharma

Abstract

The advent of the internet age and the cyberspace has proved to be a boon for all humanity, but like all novel advances nowadays, even the internet has brought about new problems that have to be addressed and handled properly in the interest of the public. Crimes that did not exist before the existence of the cyberspace have to be codified into proper offences so that the accountable individuals can be held responsible for their actions. Cybercrimes have a significant detrimental influence on our society, economy, and businesses since, for our society, it threatens our very existence. Every country has their own type of cyber-security laws that govern the use and misuse of internet and cyberspace in their respective territories, and for India, it is the Information Technology Act 2000. The current study discusses the various cybercrimes that have emerged in the current technology savvy era along with how the IT Act punishes such offences.

Keywords: Cyberspace, cybercrimes, IT act, offences

INTRODUCTION

The recent massive developments in the technological field have led to the advent of the internet age in this global era, leading to the birth of the cyberspace. Cyberspace is the notional space where computer network communication takes place. Additionally, like all different types of structures, even cyberspace needs security to protect itself from unauthorized access. This is where the concept of cyber security and cybercrimes comes in. Cybercrime may refer to any illegal or immoral act committed online or using a tool such as a computer whereas cybersecurity is the use of technology, processes, and controls to guard against cyberattack on systems, networks, programs, devices, and data. The purpose of the current research work is to examine different types of cybercrimes that are categorized under the ambit of the Information Technology Act of 2000.

Cyber law is defined as a law governing body for all legal matters relating to the internet, computer systems, cyberspace, and information technology, and the IT Act of 2000 is India's current cyber law. Cyber laws are important legal structures which are required to deter individuals from committing cybercrimes in the cyberspace. The IT act along with various provisions of the Indian Penal Code also penalize cybercrimes in India.

*Author for Correspondence

Indrayudh Chowdhury
E-mail: IC7528@bennett.edu.in

Student, Department of Law, Bennett University, New Delhi, India

Received Date: December 30, 2022
Accepted Date: March 17, 2023
Published Date: March 30, 2023

Citation: Indrayudh Chowdhury, Nimish Sharma. A Discussion on Cybercrimes with Reference to the Information Technology Act, 2000. National Journal of Cyber Security Law. 2023; 6(1): 15–21p.

In context of the present study, cybercrime refers to various acts like Hacking, Data Theft, Phishing, E-fraud, Child Pornography, Cyberbullying, etc. The researchers would analyze these cybercrimes in the context of the IT Act, highlighting the various important provisions and the punishment laid down under it, along with various landmark case laws pertaining to cybercrimes. The research methodology used by the researchers in the present study is the qualitative method, selected for its exploratory nature of its subject.

CYBERCRIMES WITH RESPECT TO INFORMATION TECHNOLOGY ACT, 2000

The following cybercrimes are some of the offences that have been described under the IT Act and have been discussed by the authors in the following papers:

Child Pornography or Material involving Sexual Abuse of Children (CSAM)

In its most basic form, child sexual abuse materials (CSAMs) refer to any media featuring pornographic pictures in which the kid being victimized or abused is visible. In accordance with Section 67(B) of the Information Technology Act, the electronic publishing or transfer of content portraying minors engaging in sexually explicit conduct is illegal:

- a. Publishes, or causes to transmit, anything in any digital form depicting minors engaging in explicit sexual acts or conducts,
- b. Generates text or electronic pictures, gathers, searches, downloads, promotes, sells, swaps, or publishes anything showing minors in an indecent or immoral or explicit sexual way; or
- c. Creates, persuades, or convinces a minor to engage in an explicit sexual behaviour or act which may outrage a rational adult using a computer, or
- d. Encourages child sexual abuse via internet, or
- e. Records personal abuse or the actions of others involving explicit sexual acts with minors in just about any digital form.

The first conviction for this offence is imprisonment for a year which may extend for a term of 5 years and include a fine which extends up to Rs. 10 lakh. The second conviction for this offence includes imprisonment of a term of 7 years and fine up to Rs. 10 lakh.

Cyberbullying and Stalking

When someone harasses or intimidates other individuals by using electronic devices like computers, mobile phones, and laptops, this is a kind of bullying known as cyberbullying. Bullying that takes place through the exploitation of digital technology is referred to as cyberbullying. It is possible that the use of portable devices, conversation networks, entertainment platforms, and social media platforms will be required. Quite frequently, this involves carrying out a number of procedures with the intention of frightening, angering, or humiliating the target. When an individual uses the Internet and other forms of technology to harass or follow another person, this behaviour is referred to as cyberstalking. Cyberstalking may take place through a variety of channels such as mails, tweets, and postings on social networking platforms, and it is typically continuous, methodical, and planned.

According to the report titled "Digital Exploitation of Children", which was produced by Ministry of Women and Child Development, the punishment for cyber cyberbullying stalking of women is outlined in sections 354A and 354D of the Indian Penal Code. The Criminal Procedure (Amendment) Act of 2013 added a new section to the Indian Penal Code (IPC) that made it illegal to engage in the practise of cyberstalking against women. Section 354D was added to the IPC. The wording of Indian Penal Code Provision 354D makes it abundantly obvious that it criminalises the conduct of stalking in both in person or by using a medium of internet equally, without making any distinctions on existence or absence of the term 'cyber'. Whereas subsection (2) of such act does not specify the way that the complainant can be considered to be 'stalked' or 'watched'.

In the case of State of West Bengal v. Animesh Box [1], the accused obtained Victim's personal and inappropriate photos by trying to hacking into her phone device, and blackmailed the victim by endangering to publish the explicit photos and video content to the all the areas of internet access, and then uploaded the suspect's private photos and personal video content onto a webpage that was considered to be sexually explicit. The accused was found guilty of all charges.

The court of west Bengal found the suspect guilty under the provisions of section 354A, 354C, 354D, and 509 of the Indian Penal Code as well as section 66C and 66E of the Information Technology Act.

The judge ruled that the accused had committed an offense in violation of Section 354D of the Indian Penal Code. The complainant experienced not only online stalking but also a form of severe violation comparable to 'virtual rape' due to the widely accessible video on various websites. This verdict has increased public awareness and reinforced the understanding that the issue at hand is a grave and significant one.

Online Sexual Harassment

It was once common practise to refer to sexual harassment as "eve-teasing". However, with collective efforts of Judicial courts, the parliament through their legislative branch, the Law Commission for India, NGOs, and female's activists, the way in which sexual misconduct of women is handled in India has undergone a significant transformation. The passage of the Sexual Harassment of Women at Workplace, Act 2013 (also known as the "POSH Act") has sent a powerful signal that every type of sexual misconduct of women in the workplace will not be considered acceptable. The act was passed in an attempt to prevent, preclude, and provide remedy for such behaviour. In addition, there has been a number of significant revisions made to the Indian Penal Code, the Criminal Procedure Code of 1973 and the Indian Evidence Act, all of which make it easier to bring charges of sexual harassment. The charge of sexual harassment was given a more severe punishment when Section 354A of the Indian Penal Code (IPC) was added which was punishable with imprisonment for a term of 3 years and fine or with both. In addition, the act of showing pornography may also be punishable by a fine.

Using an internet network to constantly call, send inappropriate messages or emails, make inappropriate conversation, or be dominant on a woman to start engaging in relationship or to develop consensual sex is an example of online sexual misconduct. Other forms of online sexual misconduct include using a computer to make inappropriate advances toward a woman. Nevertheless, personal contact or physical approaches are confined under Section 354A of the IPC; as a result, harassing an individual through an electronic medium will not fall within the scope of the IPC.

Online Job Fraud

An online job fraud program misleads jobseekers by luring them with the promise of better-paying positions and by encouraging false sense of hope. On March 21, 2022, the Reserve Bank of India issued a warning about employment scams. In doing so, the RBI had highlighted how online employment scams are perpetrated, in addition to the precautions which the ordinary job applicant in India or elsewhere should undertake. The person who is the victim of a work-from-home fraud, cyber law provides with remedies. If the fraudsters utilize your confidential information to create phoney accounts and perpetrate offences, they are accountable for Cyber Personation under Section 66-D, which is punishable offence with imprisonment of a term of 3 years maximum and a fine. The identity thieves are responsible for Identity Fraud under Section 66-C those who utilise your passcode or any other distinctive identifier.

Section 43 of the IT Act makes unauthorised access a crime, and Section 43 A holds a company accountable for invasion of confidentiality and privacy by compensating the complainant for failing to secure their information. The information you supply to con artists is invaluable. Alongside your private details, fraudsters also possess and exploit your credit card details. When purchasing a welcome package, users might not even be sent to a secure payment gateway. This makes you susceptible to credit card theft. And your personal information is transferred to marketing firms outside the purview of your permission and approval.

Internet Extortion

Cyber criminals engage in digital sextortion when they threaten to divulge sensitive and private data via digital means. These criminals use threats to get a person's sexuality, bodily favour, or money. The Punishment for breach of privacy and confidentiality has been stated under Section 72 which states that any individual who, in furtherance of this act, has obtained access to any online database, journal,

record, communications, details, written statement, or other information without the consent of the individual concerned and reveals such content to another Individual without the permission of the concerned individual is subject to imprisonment not exceeding the term of 3 years. This section applies to any individual who has obtained accessibility to any online database, journals, record, communication, data, document, or other information as per the powers granted by the IT Act or its related regulations and rules. If this individual divulges such data, he will be penalised. It would not apply to the disclosure of an individual's personal details by a webpage or mail provider. The punishment for this offence is imprisonment up to 2 years in jail or liable for a fine of maximum up to 1 lakh, or with both.

Phishing

Phishing, which occurs when a person is impersonating someone online in order to get access to sensitive information, has been recognised as being one of the absolute cheapest methods employed by criminals. Phishing consists mostly of one person delivering a false and misleading communication to the other while posing a trustworthy source in order to get confidential material. Phishing's primary purpose is to steal private data or attack the victim's machine with virus. This includes fake emails and SMS messages issued in the guise of a company to get credit card details.

Phishing occurs when an unknowing victim clicks on a fraudulent email, link, or other means of communication that appears to have been issued by a trusted individual or organization. In accordance with the Information and Technology Act of 2000 ('IT Act') phishing is a cybercrime since its main object is to steal sensitive information from another person by impersonating other person. The crime-related elements were incorporated with the 2008 amendment. The provisions that incorporate and regulate the crime of phishing vary across jurisdictions, but commonly include laws related to fraud, identity theft, cybercrime, and unauthorized access to computer systems. These provisions aim to address and prosecute the act of phishing, which involves fraudulent activities aimed at deceiving individuals and obtaining their sensitive information.

Data extraction or Access without Authorization

A person is liable under section 43 of the Act if any individual acquires unauthorized access to computer network or computer system of another user with the intention of downloading, accessing, disrupting, denying, or corrupting the data contained within.

In case, Poona Auto Ancillaries Pvt. Ltd, Pune V. PNB, New Delhi & Ors [2], a fraudster transferred around Rs. 8.10 lakh from MD of the Firm (Mr. Manmohan Singh Matharu) from PNB bank by a phishing email which was responded by the complainant which resulted in sharing the liability of such money transfer. Though the bank was held negligent for their poor security checks which led this fraudster to transfer the money.

Penalty of Phishing

Section 66 of the IT Act specifies the penalties that can be imposed on phishers who steal the account information of their victims. Depending on the gravity of the offence, the punishment includes imprisonment that can exceed a term of 3 years or liable for fine that may extend up to Rs. 5 lakhs, or with both. In case, Kumar V. Whiteley [3], the accused was held liable to unauthorised logging in to the BSNL Broadband and modifying the databases of the computer which was linked to the broadband. After investigation by CBI, Kumar's conduct was held in violation of Section 420 of IPC and Section 66 of IT act by the magistrate with a year of imprisonment and Rs. 5000 fine.

False Information Dissemination

The provision Section 66A specifies that the dissemination of false information with the goal to cause harm to the victim is punished. In addition, the provision specifies the offences that will result in the required punishment.

Section 66 C

The rules of this section prohibit the use of passwords, electronic signatures, and any other unique identifier for any individual. Phishers engage in fraudulent activity while posing as the legitimate account holder and committing fraudulent acts.

Identity Theft

Under the requirements of section 66D, impersonating another person while using communication devices or computer resources is considered cheating. Fraudsters impersonate banks and other organizations by employing URLs that lead customers to fake copies of the real websites, creating the appearance that they are affiliated with the same organization. In addition, Section 81 of the Act contains an obstante clause, meaning that the provisions of the IT Act will take precedence and supersede those of the existing framework. However, it is also vital to note that phishing scams are bailable under Section 77B of the IT Act (Amendments 2008).

In case, *Shreya Singhal v. Union of India* [4], the validity of Section 66A of the IT Act was questioned on the basis of article 19(1)'s guarantee of freedom of expression (a). The provision made illegal the broadcast of misleading info with the intent to injure the victim. The Supreme Court decided that Section 66A of the Information Systems Act breaches article 19(1)(a) of the Constitution because it creates an environment in which the basic act of speaking and deliberating is repressed (chilling effect).

In accordance with article 19(2) of the Constitution, the court concluded that the provision did not fall under the exclusions since the terms "annoy, inconvenience, or offend" are vague. In addition, it was remarked that the vague and unenforceable aspect of the exclusion will restrict freedom of expression in the nation. The court deemed Section 66A of the IT Act invalid based on this reasoning.

Obscenity

The IT Act's Sections 67, 67A, and 67B detail the penalties for publishing or transmitting in electronic format:

1. obscene material;
2. material containing sexually explicit acts, etc.; and
3. material depicting children in sexually explicit acts, etc.

For a first conviction, Section 67 of the IT Act mandates 3-year term imprisonment or a fine up to 5 lakh and for a second conviction, imprisonment up to 5 years term or a fine of up to 10 lakh.

In the case, *The State of Tamil Nadu v. Suhas Katti* [5], wherein the matter was regarding a divorced lady involved the publication of defamatory, obscene and abusive statements in a Yahoo chat group. Using an e-mail account created by the offender in the name of victim, the accused forwarded information-seeking e-mails to the victim. These ads resulted in the lady receiving several annoying phone calls. The suspect was captured by the police in response to the report. He was a prominent member of the victim's family who intended to marry her. She married other person, however the relationship ended in divorce. The accused then re-established communication with her. As a result of her refusal to marrying him, he started to abuse her through the Internet.

The defendant was convicted and punished as follows for violation of sections 67 of IT Act, 469 and 509 of the IPC Act. "The defendant is found to have violated sections 469, 509, and 67 of the Information Technology Act of 2000. The defendant is convicted and punished for the violation of section 469 IPC to 2 years of RI and a fine of Rs. 500, and for the violation of section 509 IPC to 1 year of simple imprisonment. The offender was detained at Central prison of Chennai and was held liable to pay fine. This was the first instance in India in wherein section 67 of the Information Technology Act of 2000 was applied.

Penalty for Privacy Breaches

Section 72 states: "Except as otherwise provided in this Act or any other law in force, any person who, in pursuance of any of the powers conferred by this Act, rules or regulations made thereunder, has obtained access to any electronic record, book, register, correspondence, information, document, or other material without the consent of the person concerned and discloses such material to any other person shall be punished with imprisonment for a term not exceeding 1 year." Such Term maybe extended up to imprisonment of 2 years or may be liable for fine up to Rs. 1 lakh or both.

Cyber Terrorism

The Information Technology Act, 2000 criminalises cyberterrorism under Section 66F of the code. That whoever, with the intension to endanger the unification, honesty, safety, or sovereign rights prevalent under law, or to induce fear to individuals or any segment of individuals, tries to deny or causes the denying access to an individual who is authorised to access a work computer, or attempts to penetrate or connect directly a network of computer without permission or accessing system users, or exposes or induces the data of any computer system, and through such behaviour causes or is responsible for any loss or harm, shall be punishable with imprisonment. Whoever acts or colludes to conduct cybersecurity threats will be sentenced to life in prison.

Computer Manipulation and Tampering

In accordance with sections 43(h) and 66 of the IT Act, anybody who credits the operations of another individual to his account by altering or interfering with a system, computer, or computer network is subject to punishment. A person who tampers with an electrical provider's computer system and forces his friend to compensate for his power use would be punished under section 43(h) of the Information Technology Act, which does not appear in the IPC.

CONCLUSION

The advent of the internet age has led to the development and increase of cybercrime in society. Numerous types of new crimes which were not even conceivable in pre-internet days have to be addressed now to ensure justice and fairness. The current study discusses the various cybercrimes that have been addressed by the Cyberlaw existing in India. Proper legal structures and legislations are required to control and deter people from this criminal aspect of the cyberspace.

However, like all different types of environments, layman individuals who do not understand the intricacies of the cyberspace have a duty to be protected by the policies of their government. The IT Act has come a long way to fill this requirement, but it is not enough. There are still numerous gaps left behind in the IT Act and different types of cybercrimes still exist which are not easy to track. Detailed provisions are need to be added frequently in the Cyberlaws to keep level with new cybercrimes which pop up every day. Inadequate literacy about the cyberspace, cybersecurity and cybercrime also plays a huge role in undermining security in the cyberspace. Governments should take the initiative to educate the people and make them aware about their rights and responsibilities related to the cyberspace. Proper utilization of knowledge would arm the people and help them in protecting themselves from the dark aspects of the internet.

Abbreviations

Abbreviation	Full Form
IT	Information Technology
IPC	Indian penal Code
CRPC	Criminal Procedure Code
CSAM	Child Sexual Abuse Material
NGO	Non-Government Organisation

V. Versus
S. Section

REFERENCES

1. State of West Bengal v. Animesh Boxi, GR No. 1587 of 2017.
2. Poona Auto Ancillaries Pvt. Ltd, Pune V. PNB, New Delhi & Ors., Cyber Appeal/4/2013, Misc Application/12/2018.
3. Kumar V. Whiteley, [1991] 93 Cr. App rep 25.
4. Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73.
5. State of Tamil Nadu v. Suhas Katti, C No. 4680 of 2004.