National Journal of
Cyber Security Law

ISSN: 2582-9750
Volume 6, Issue 1, 2023
DOI (Journal): 10.37591/NJCSL

http://lawjournals.celnet.in/index.php/njcsl/index

Review NJCSL

Cyberlaw in India

N. Venkat Abhinav, Ananya Paliwal*

Abstract

Cyber law is a branch of law that governs the use of the worldwide web, cyberspace, and digital communication and data systems. With the advancement of technology as well as the internet, cyber law has become essential in safeguarding people, companies, and organizations from computer crimes, cyber-attacks, and data leaks. Cyber law encompasses a wide range of legal issues, including online privacy, digital transactions, data security, cyber warfare, cyberbullying, hacking, and intellectual property violation. The goal of cyber law is to create regulatory structures and laws that govern how information technology and the web are used and protected. The internet has drastically changed the way we interact, operate a business, and access information. Nevertheless, these improvements have led to a rise in cyberattacks, including identity fraud, online abuse, and cyber warfare. Cyberlaw plays an important role in combating these risks by providing victims with legal recourse and imposing penalties on offenders. Cyberlaw requires a collaborative effort from legal experts, policymakers, and technology professionals. Governments and international organizations have passed legislation to protect internet privacy, establish streaming rights, and guarantee a secure and private cyberspace. Furthermore, businesses and organizations must follow cyber laws in order to safeguard their client's data and information. Cyber law is an essential component of our digital society, and its significance will only grow as technology advances. To protect ourselves from the growing threats in cyberspace, we must have a solid understanding of cyber law. Effective cyber law implementation is a collective responsibility that necessitates a collaborative effort from individuals, businesses, governments, and technology professionals.

Keywords: Cyberlaw, world wide web, cyberspace, communication and data systems, computer crimes, cyber-attacks, data leaks

INTRODUCTION

Cyberlaw

Cyberlaw, also known as internet law, is an area of law that deals with the connection the Internet has, with technological and electrical factors such as computers, programs, technical infrastructure, and information systems. It protects data exchange, confidentiality, telecommunications, copyrights, and free speech when accessing the Web, computers, cell phones, and so on. As Internet traffic has increased, so has the proportion of legal issues raised around the world [1]. As cyber laws vary by jurisdiction and country, it is difficult to enforce them, and the punishments for violation can range from fines to imprisonment for years.

***Author for Correspondence**
Ananya Paliwal
E-mail: ananyapaliwal.student@slsnagpur.edu.in

Student, Faculty of Law, At Symbiosis Law School, Nagpur, Maharashtra, India

Received Date: February 16, 2023
Accepted Date: March 22, 2023
Published Date: April 05, 2023

Citation: N. Venkat Abhinav, Ananya Paliwal. Cyberlaw in India. National Journal of Cyber Security Law. 2023; 6(1): 8–14p.

Because it includes all the aspects of online operations and interactions that happen on websites, the internet in general, and its various means, Cyber law is critical and essential in our everyday lives. Every online action and reply also has legitimate consequences.

History of Cyber Law in India

The UN general assembly on January 30th, 1997 passed the information technology act through a

resolution, in which the Proposed Legislation on E-commerce for international trade laws was endorsed. This resolution suggested, among other things, that all the countries give this legislation favourable regard when updating and adopting their new laws so that uniformity might be maintained in relevance to paper-based communications and data storage.

The Department of Electronics (DoE) implemented this bill in July 1998 [2]. However, it was not presented to the House till almost a year and a half later, when a fresh IT Department was established. The Trade Ministries made proposals concerning trade and WTO scores, which dramatically impacted it. The Ministry of Justice and Corporate Relations also looked into this common issue.

After many members requested, the bill was submitted to the 42-member standing committee following its submission in the House. The Committee submitted many adjustment proposals to the current measure. Nevertheless, only recommendations that had been accepted by the Department of IT were taken into consideration. One of the more popular recommendations that were highly debated was that an internet café owner should maintain a register with the addresses and phone numbers of all the customers, in addition to a record of the websites they accessed.

This proposal was created in order to prevent cybercrimes and facilitate the speedy recognition of a fraudster. During the same time, it was inspected because it would venture into a cybersurfer's sequestration and would not be financially sustainable. The IT Department ended up dropping this idea in its final draft. The proposal was agreed upon by the Cabinet of ministers on May 13, 2000, and both houses of the Parliament enacted it on May 17, 2000. On June 9, 2000, the President approved the bill that then it became to be known as the Act on Information Technology or the IT Act 2000. The Act came into force later on October 17 of the same year.

Cyber Law Acts in India

In India, cybersecurity rules and regulations are specified in the IT Act, of 2000. The fundamental purpose of this Act is to legalize virtual trade and make it easy to submit electronic documents to the government. Acts, Rules, and guidelines that come under the purview of cyber laws include:

1. The IT act, 2000.
2. Certification of Authorities Rules, IT 2000.
3. Security Procedure Rules, IT, 2000.
4. Certification of authorities Regulations, IT 2000.

In India, there is no specific legal structure for cyber law. It integrates laws governing agreements, copyrights, data security, and confidentiality. With the internet and computers pervading every aspect of our life, tougher cyber legislation is required. Cyber laws govern various digital exchanges, programming, data security, trade, and banking operations in our day-to-day lives.

IT act of 2000 makes a wide range of cybercrimes illegal. Information technology, smartphones, malware, and the internet serve as both a gateway and a victim for this type of criminal conduct. On the internet, all typical criminal behaviours such as robbery, deceit, fraud, slander, and damage are carried out. These concerns are already addressed in the IPC.

WHAT IS A CYBERCRIME?

Cybercrime is described as any illegal activity taking place over a computer, a network resource, the internet, or including any of these platforms in performing such activity. Whereas most cybercrimes are performed for profit, other cyberattacks/crimes are done against computers or electronic equipment with the goal of harming or disabling them.

Categories of Cyber Crime

Cybercrime is divided into three major groups. They are as follows:

1. *Crimes in relation to Persons:* Although a majority of these offenses are committed digitally, they have real-world impacts. Such crimes include cyber harassment, stalking, various types of

impersonation, financial fraud, data breaches as well as the distribution of sexually explicit material, etc.

2. *Property-related offenses:* Most of these online crimes involve theft or loss of property, like a computer or a server. DDOS attacks, hacking, computer vandalism, intellectual property theft, and other such breaches are examples of these crimes.
3. *Crimes in relation to the Government:* When a cybercrime is committed against a state, it is considered to be an attack on the nation's privacy as well as is considered a war crime. It includes hacking, collecting sensitive data, cyber warfare, and internet fraud.

WHAT IS A CYBER ATTACK?

A cyber-attack is something that occurs when an unknown third party obtains access to a networked system. A hacker is the one who carries out this attack. Cyber-attacks have a variety of negative repercussions. Whenever such an attack is carried out, security breaches occur, which can lead to information loss or deception. Organizations incur huge financial losses and lose reputations and customer trust as a result of this.

Types of Cyber Attacks

There are several forms of cyberattacks in today's world [3]. The following are the 10 most common cyber-attacks that, based on their scale, can severely harm a person or an organization:

- *Malware Attack:* This type of cyberattack is extremely common. Malware refers to the usage of various malicious software viruses like worms, adware, ransomware, etc. Malware infiltrates a network by taking advantage of a single defect. It begins whenever a user clicks on a malicious link, then it downloads an unsolicited email attachment, or uses an infected USB device to further corrupt the device.
- *Phishing Attack:* Phishing is among the most common types of cyberattacks. It is a social manipulation attack where the hacker adopts the identity of a trustworthy acquaintance and sends misleading and fraudulent email messages to the victim. Without identifying it, the victim opens these e-mails and clicks on the URL or unintentionally downloads an attachment. As a direct consequence, the hackers gain unauthorized direct access to the victim's private information as well as their login credentials. This same procedure can also be used to install malware.
- *Password Attack:* An example of this type of attack is when a hacker uses multiple passcode-breaking apps and tools to penetrate into devices' software, like Aircrack, and Hashcat, among others. This kind of attack can be further split into three different kinds: dictionary attacks, brute-force attacks, and keylogger attacks.
- *Man-in-the-Middle Attack:* Also known as an eavesdropping attack, it is when a hacker intervenes between two parties, for example, when a hacker intercepts and manipulates a conversation between a client and a host. The hacker then steals and modifies the data in a manner of his choice. The communication line between the parties is then terminated, and this line now runs through the scammer.
- *SQL Injection Attack:* A Structured Query Language injection attack occurs when a hacker creates a bogus SQL query on a database-powered website. It is accomplished by implanting a malicious code into an unencrypted web page search field, causing the server to unveil sensitive information. As a result, the hacker can read, update, and remove entries in the databases. Through this, hackers might even obtain admin access to these databases.
- *Denial-of-Service Attack:* In this scenario, hackers identify and target specific systems, data centres, or connections and flood them with traffic, reducing their potential and connectivity. When this occurs, the servers become overloaded with incoming client requests, causing the site and its hosts to stop working or slow operations. As a result, inquiries that are actually valid go unanswered. When hackers combine numerous hacked systems to launch an attack like this, it is referred to as a Distributed Denial-of-Service attack.
- *Insider Threat:* As the term implies, an insider threat concerns an internal entity instead of an external party. In such a case, it could be someone from within the organization who is intimately

familiar with every detail of the organization. Insider threats have the potential to cause significant damage. Because employees are granted access to many accounts containing sensitive information, insider threats are common in small businesses. This type of attack can be motivated by a variety of factors, including avarice, malice, or even negligence. Insider threats are difficult to foresee and thus handle.

- *Cryptojacking:* Cryptojacking occurs when a hacker gets access to another person's device in order to mine cryptocurrency. The hacker gains access by breaking into a webpage or defrauding the individual into clicking on a rogue link. They use web infomercials with a specific JavaScript code to achieve all this. Victims are uninformed of this because the code operates in the background; the only indication they may see is a delay in performance.
- *Zero-Day Exploit:* A Zero-Day Attack occurs after the disclosure of a networking vulnerability; in most cases, there is no solution. As a result, the company informs customers about the flaw; however, this information also reaches hackers. The developing company may take any amount of time to fix the issue depending on the weakness. Meanwhile, hackers are focused on exploiting these weaknesses. They ensure that it is exploited before any solution is executed.
- *Watering Hole Attack:* The victim in this instance is a small subset of a big organization, region, etc. In this form of attack, the hacker aims at websites frequented by the selected target group. Websites are found either by closely checking this group or speculating on their actions. Following that, the hackers infiltrate such websites using malware, that infects the equipment of the victims. In such an assault, the malware attacks a user's personal data. In this case, the hacker may also receive a remote connection to the infected system.

BIGGEST CYBER CRIMES IN INDIA [4]

- *SBI data breach, January 2019:* A security analyst reported, completely anonymously, that the nation's biggest bank, State Bank of India, failed to use a password to secure a server. SBI Quick was a service that sent clients text messages with their recent activity and current account balance details. Customers received almost over 3 million text messages from the bank.
- *Just dial data breach April 2019:* JustDial is a search engine tool that supplies you with data about everything. In April 2019, more than 100 million customers' data was exposed and publicly disclosed. The information contained names, contact information, mailing addresses, birthdates, genders, and addresses. An anonymous security trainee disclosed this in a post on Facebook.
- *Health record breach August 2019:* FireEye is a business security company. Hackers infiltrated and stole data of over 68 lakh patients and physicians out of an Indian health services website, according to the company. According to FireEye, the intrusion was carried out in China by a hacking organization known as Fallensky519. The group sold these health care records mostly on the dark web, and various patient and physician records were accessible for USD 2000.
- *Unacademy data breach May 2020:* Unacademy was formed in 2015 for developing online education and had received funding from giant investors including Facebook Sequoia India etc. The corporation stated that a cyber breach has occurred, compromising the identities of over 22 million registered members on their website. Cyble, a cyber security firm, disclosed that data such as names, email accounts, and credentials were sold on the dark web.
- *Big basket for sale on the dark web October 2020:* Big Basket is an online grocery delivery service. Big Basket had been listed for sale over the dark web, according to cybersecurity agency Cyble. In addition, a portion of its massive database containing the personal information of nearly 20 million customers was made accessible for USD 40,000. On November 1, Cyble authenticated all data that was available for sale of Big Basket and notified this breach to Big Basket. The information contained names, PINs, phone numbers, email accounts, birthdates, IP addresses, and whereabouts.
- *Juspay to Sale on the Dark Web January 2021:* Juspay is a digital money transfer system that was created especially for mobile transactions. Juspay disclosed in January 2021 that a server containing disguised credit data and card biometrics of 35 million users had been compromised. This non-recycled login key was used to breach the information. According to cyber security

researcher Rajshekhar Rajaharia, the information was scheduled to be sold on the darknet for USD 5000.

- *Covid-19 Test Results of Indians Leaked in January 2021:* The Indian authorities released the Covid-19 lab test findings of approximately 1500 Indian patients. Alarmingly, the material was not sold on the black market but was then released to the public as a result of Internet indexing. Several documents were published on the portals of government entities that were using "gov.in" subdomains. These agencies were eventually discovered to be in New Delhi. The disclosed information included names, birthdates, test dates, and the centres.
- *Police Exam Applicants data February 2021:* Over 500,000 registrants' personally identifiable data connected to their personality was made available for purchase on databases sharing websites. CloudSEK, a threat detection company, traced it. The information was traced all the way back to an Indian army exam held in 2019. CouldSEK received data on over 10,000 applicants from the seller. The information exchanged included the candidates' names, birthdates, email accounts, telephone numbers, FIR reports, and criminal histories. Following the investigation of this leaked information, it was discovered that the majority of the applicants were all from Bihar. When the threat-intelligence firm compared the mobile numbers to the candidates' names, it was discovered that the stolen data was genuine.
- *Upstox Reset Passwords April 2021:* Upstox is an online trading platform based in India. The corporation admitted to a cyber compromise of KYC records in April 2021. Because these records could be used by hackers to steal identities, financial service providers acquired them to validate customers' identities and to prevent embezzlement and fraud.
  In April 2021, the company notified the clients that they would change their credentials and undertake other precautions as quickly as they received a notification in an anonymous mail that the client addresses and KYC data stored in one third-party storehouse had been stolen.
- *Domino's India April 2021:* On the online black market, data about customers from over 180 million Domino's India sales were for sale. Alon Gal, CTO of cybersecurity company Hudson Rock, exposed it. He further stated that somebody offered to get information of 13 GB of data, including 1 million customers' credit card information as well as the details of 180 million pizza purchases at 10 bitcoin, which would be worth around Rs. 4 crore. The information includes the names, email addresses, and phone numbers of the customers.
  Alon Gal tweeted an image of the hacker alleging to have details of over 250 Domino's India personnel as well as their outlook email dating all the way back to 2015. Jubilant Foodworks, the holding company of Domino's India, confirmed this data leak to IANS but disputed that the customers' payment information had been stolen because they do not keep credit card data.
- *Air India Cyber Breach May 2021:* Air India's database was hacked in May 2021, compromising the personal information of approximately 4.5 million travellers. The hacked data was gathered between August 2011 and February 2021. SITA, the aviation information service supplier, disclosed this issue. Passengers were not informed of the event until March. This attack on SITA's passenger service system impacted not only Air India, but also many other airlines [5].

THE NEED FOR CYBER LAW

Cyber Law is flourishing diligence in India and is acknowledged to be one of the most significant pieces of legislation of the 21st century. It is an emerging subject in India with tremendous potential for expansion and diversification.

This law was created in India with the help of a multitude of diverse multinational agreements and treaties. The fundamental goal of Cyber Law is to regulate and control the various electronic transactions. There are multitudinous benefits to Cyber Law in India. It helps to create businesses in the country and offers formal protection for digital means. It also offers vittles for Indian e-commerce policies. These laws also help to prevent computer-related offenses. It also has tools for monitoring the internet as well as other internet technology. India's cybersecurity laws also contribute to the growth of the country's digital infrastructure. Cyber Laws in the country also help to prevent computer as well as

other electronic gadget abuse. It also helps to prevent unwanted access to information systems and networking. They also aid in the expansion of electronic services in the country.

The importance of cyber legislation in India arises from the fact that the cybersecurity acts in India incorporate and encompass all aspects of what happens on or with the internet, from small transactions to any big activities involving the internet or cyberspace in general.

Evolution of Cyber Law in India

The rising dependence on technology highlighted the necessity of cyber law. Dependence on advanced technologies has both its benefits and drawbacks. The beginning of the 21st century witnessed the establishment of cyberlaw in India with the IT Act of 2000 [6].

The following is the concept of India's Information Technology Act:

- Ensuring that all transactions are fairly honoured.
- To fete digital autographs as valid autographs to accept agreements online.
- Giving legal recognition to bankers and other associations who maintains accounting books in electronic form.
- Cybercrime forestalment and online sequestration protection.

The Indian IT law streamlined both the RBI Act and the Indian telecommunications Act. Nearly all online conditioning has come under scrutiny as cyberlaw has evolved. Still, when it comes to cyber law, there are some areas where cybercrime laws in India do not apply, similar to:

- Negotiable Instruments excluding cheques,
- Legal Representation,
- Equity,
- The contract for the sale or transportation of an underlying asset, and
- Notified documents, and deals are done by the union government.

Future of Cyber Law

A number of elements, including increased technological use, globalization of the economy, and the rising risk of cybercrime, are expected to impact the evolution of cyber laws in India:

- Almost definitely, technologies will remain to play a significant role in the growth of cybersecurity laws in the country. Using of smartphones, the internet, and cognitive computing are all likely to increase, posing new difficulties and possible scenarios for the legal system.
- The development of these laws in the country will very certainly be influenced by increasing globalization. As organizations grow to get bigger and bigger, they would indeed be subject to a multitude of policies and guidelines. Businesses will need to take a more sophisticated approach to legal compliance as a result of this.
- Cybercrimes are also likely to increase in the future. Attacks by hackers are growing increasingly clever, and the risks are escalating. As a consequence, both huge companies and individuals would have to be more cautious in combating these cyber criminals [7].

CONCLUSION

Cyberlaw is constantly evolving to keep up with the ever-growing developments on the internet and in technology. Despite the fact that laws may occasionally fall behind the pace of technology, it is crucial for people to be aware of their rights and obligations when taking part in online activities. This includes being aware of how to protect themselves from cybercrimes and respecting other people's online rights. Finally, because cyberlaw is a rapidly evolving field, it is critical for people to exercise caution and keep up with current events so as to protect themselves better from this virtual hazard.

REFERENCES

1. Indian cyber security. (2023). History of cyber law in India [Online]. [cited 2023 Mar 29]. Available from: https://www.indiancybersecurity.com/cyber_law_history_india.php

2. Legal service India. (2013). Importance of Cyber Law in India [Online]. [cited 2023 Mar 29]. Available from: https://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html
3. Fortinet. (2022). Cyber Glossary guide and definitions. [Online]. [cited 2023 Mar 29]. Available from: https://www.fortinet.com/resources/cyberglossary
4. Policy bazaar. (2021). Biggest Cyber Breaches in India [Online]. [cited 2023 Mar 29]. Available from: https://www.policybazaar.com/corporate-insurance/articles/biggest-cyber-breaches-in-india/
5. Hindustan times. (2021). Air India data breach: All you need to know [Online]. Hindustan Times. [cited 2023 Mar 29]. Available from: https://www.hindustantimes.com/india-news/air-india-data-breach-all-you-need-to-know-101621647788771.html
6. Tax guru. (2012). Overview of cyber laws in India Index. [Online]. Available from: https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf
7. ET CIO. (2023). Cyber Law News. [Online]. ETCIO.com. [cited 2023 Mar 29]. Available from: https://cio.economictimes.indiatimes.com/tag/cyber+law

