DE JURE NEXUS LAW JOURNAL

Author:

Sourika Jana

Symbiosis Law School, Noida

2nd Year, BA LL.B.

ANALYSIS OF INDIAN CYBER LAWS AND CRIMES

Abstract

Cyber laws and crimes in India fall within the jurisdiction of the Information Technology Act. In the digital era, with billions of internet users, it becomes difficult to safeguard the user's rights ethically, the IT act provides a comprehensive solution. This paper starts with a brief introduction to the developmental history of cybercrimes. It also discusses the landmark cases related to cyber-crimes which led to the changed in the way people perceived the internet and its precautionary measures. The IT act demonstrates the different types of cyber-crimes that someone can fall victim to like crimes against individuals, property, organizations, and society. The Indian penal code in association with the IT act is responsible for safeguarding the citizen's interests. For crimes like data theft and identity theft, the law penalizes the accused with imprisonment for 3 years. Despite the aforementioned benefits, there is a need for stricter implementation and rigorous punishment for cybercriminals as the injury they cause can result in lifelong damage.

Historical Background

The first cybercrime is thought to have occurred in the year 1820. This is supported by the fact that computers have existed in India, China, and Japan since 3500 BC. Charles Babbage's analytical engine was the forerunner of the modern computer.

Banks and other financial organizations were among the private sector's earliest large-scale computer users, automating payroll and accounting processes. As a result, fraud in a computer scheme came together. The equity-funding Corporation in the United States was one of the earliest examples mentioned as an example of computer-related fraud. The fraud was straightforward. Because auditors and regulators regarded computer printouts as authoritative evidence of policy rather than asking for actual paperwork, the scams were successful. When the scam was detected, 64,000 of the 97,000 policies supposedly issued by the firm turned out to be fraudulent, resulting in a loss of nearly 1 billion pounds.

Morris Worm gave way to ransomware in the world of cybercrime. Many countries, including India, are striving to prevent such crimes but the nature of these attacks is ever-changing and difficult to ascertain.

As social networks became more prominent, the rate of cybercrime began to rise as thieves gained easier access to the user's personal life. As a result of this progression, one of the most heinous kinds of criminality emerged: **non-consensual sharing of intimate images (NCSIA).** In 2015-2016, 569 instances out of 5987 cybercrime cases were motivated by sexual exploitation, according to the **National Crime Record Bureau (NCRB)**. In such situations, indecent photos of the victim are posted on the internet without the victim's knowledge or agreement. It's also known as non-consensual pornography.

De Jure Nexus LAW JOURNAL

According to NCRB statistics, the distribution of such photos on the internet has grown by 104 percent in recent years. Most of these incidents go unreported because the victim's family does not want to violate their privacy or become involved with the police and courts, and the victim prefers to keep such cases to themselves for fear of being shamed. The perpetrator is aware of these realities and exploits them. This is a crime that may traumatize whoever is victimized, whether it's a major star, such as Hollywood actress Bella Thorne, or a regular girl. It is a major issue in India, which we should be concerned about because no specific laws are dealing with such crimes. Perhaps since the majority of incidents go unreported, legislators are unaware of the severity of the crime. If such a situation arises, we have a few laws under the **Indian Penal Code (IPC)** and the **Information Technology Act 2000** to help us deal with it.

No one has been spared by cybercrime. It has a stronghold in all key industries, including banking and finance (Union Bank of India Heist (2016), commercial facilities (WannaCry Ransomware (2017)), postal services (Data Theft at Zomato (2017)), transportation, and e-commerce platforms. Phishing and social engineering, malware, spear phishing, ransomware, hacking, software piracy, pornography, cybersquatting, and other forms of cybersquatting are all examples of it. The seriousness of the problem is highlighted by a recent cyber-attack on one of India's nuclear power facilities and the Prime Minister's social media handle.

Cyber Crime's in India (Case Studies)

Bank NSP Case[1]

In this situation, a bank management trainee was engaged to be married. Using the company's computers, the pair exchanged many emails. They had split up after some time, and the young woman established some phony email ids, such as "Indian bar organizations," and used them to send emails to the boy's international clientele. She did this on the bank's computer. The boy's business suffered significant losses as a result of the bank's actions, and he brought the bank to court. The bank was held responsible for the emails sent.

Bazee.com case

(*Sharat Babu Digumatri v. Government of NCT of Delhi*)[2]

The Chief Executive Officer of Bazee.com was detained in December 2004 because he was selling an inflammatory compact disc (CD) on the website, and the CD was also sold out in the Delhi

[1] Available at: http://www.indiancybersecurity.com/case_study_the_bank_nsp_case.php, last visited on 16/08/2021, 15:32

[2] Criminal Appeal No. 1222 OF 2016

market. The Delhi police and, as a result, the Mumbai police were called in, and the CEO was eventually released on bail.

Parliament Attack Case

(*Mohd. Afzal Kumhar and Anr. v. State*)[3]

This case was handled by the Bureau of Police Research and Development, Hyderabad. The terrorist who attacked the Parliament was found with a laptop. "*The laptop taken from the two terrorists who were killed down on the 13th of December 2001 when the Parliament was under siege was submitted to the BPRD's Computer Forensics Division*."[4] The laptop contained several proofs that affirmed the two terrorists' motives, including a Ministry of Home sticker that they had created on the laptop and affixed to their ambassador's car to gain access to Parliamentary House. They created a fake ID card with a Government of India emblem and a seal that one of the two terrorists was carrying. The emblems (of the three lions) were meticulously scanned, and a seal was crafted with care, complete with a Jammu and Kashmir residence address. However, further, examination revealed that everything was forged and created on the laptop.

Yahoo Inc. Vs. Akash Arora [5]

Plaintiff owned the well-known trademark "Yahoo!" as well as the domain name "yahoo.com." Defendant bought and registered the domain name "Yahooindia.com" in his name. The Plaintiffs filed a complaint, alleging that Defendant's acts constituted 'passing off,' and that he should be permanently prohibited from doing so.

The Hon'ble Court determined that the word "Yahoo" has gained uniqueness and is linked to Plaintiff's business. Defendant's usage of the domain name "yahooindia.com" results in Plaintiff's business being misrepresented as his own, and as a result, Plaintiff's company will be affected. Hence, an injunction prohibiting Defendant from utilizing the infringed trademark was issued.

Cyberlaw

[3] Criminal Appeal No. 811 of 2007

[4] A brief study on Cyber Crime and Cyber Laws of India, Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06, June -2017

[5] 1999 IIAD Delhi 229, 78 (1999) DLT 28

Cyber Law was created to put a stop to crimes perpetrated through the internet, in cyberspace, or through the use of computer resources. Cyber Law is a phrase used to describe the legal concerns that arise from the use of communication or computer technology.

What is the importance of Cyber Law?

Cyberlaw is highly important in today's technological world. It's crucial since it affects almost every aspect of online activity and transactions, as well as other types of communication. Every action and reaction in Cyberspace are accompanied by legal and cyber legal views, whether we realize it or not.

The Information Technology Act of India, 2000

On January 30, 1997, the United Nations General Assembly passed a resolution creating the Information Technology Act, which led to the adoption of the Modern Law on Electronic Commerce on International Trade Law.

The Department of Electronics (DoE) drafted the law in July 1998. It couldn't be brought up in the House until December 16, 1999, when the new Ministry of Information Technology was created. However, it suffered some changes in the commerce business as a result of numerous suggestions related to e-commerce and worries regarding the World Trade Organization (WTO)'s obligations. After being submitted to the Parliament, the bill was sent to the 42-member Parliamentary Standing Committee in response to demands and suggestions from members. One controversial suggestion was that a cyber café owner retains a record with the names and addresses of all visitors, as well as a list of the websites they viewed.

This suggestion was made in the hopes of reducing cybercrime and making it simpler to track down a cybercriminal. Simultaneously, it was derided since it would invade a net surfer's privacy and be unprofitable. Finally, in the final draught, the IT Ministry deleted this proposal.

According to Wikipedia, "The Information Technology Act, 2000 (commonly known as ITA-2000 or the IT Act) is an act of the Indian Parliament (no 21 of 2000) notified on October 17, 2000. It is India's most important law addressing digital crimes, often known as cybercrime, and online

commerce. It is based on the United Nations Model Law on Electronic Commerce (UNCITRAL Model), which the United Nations General Assembly recommended in a resolution dated January 30, 1997."

The following are some major points from the Information Technology (IT) Act of 2000:

• E-mail is now regarded as a legitimate and legal mode of communication.

• The Act grants legal status to digital signatures.

• This Act permits the government to publish notifications on the internet using e-governance, which has provided a new economic opportunity for corporations to issue digital certificates by allowing them to become Certifying Authorities.

• The internet may be used to communicate between corporations or between companies and the government.

Analysis

Because cybercrime is such a wide subject, describing it in just one or two phrases is impossible. However, if we examine the nature of this crime, we can conclude that it is the type of crime in which computers and computer networks are exploited or misused, and the crime is done either 'through' or 'to' them, or both. Indians file 32 percent more complaints than those in the United States and the United Kingdom, according to an Ipsos poll. It is only approximately 11-15 percent in other technologically advanced countries. The 32 percent figure only applies to cases that have been documented, not to cases that have gone unreported.

Classifications of Cyber Crime

The following are the four major types of cybercrime. The specifics are as follows:

1. Cyber Crime against individuals:

   Cybercriminals target an individual or a group of individuals. Here are a few examples of individual-targeted cybercrime:

   - Email spoofing: The creation of an email header is used in this manner. This indicates that the communication does not appear to originate from the true or original source. People are more likely to read an electronic message or email

if they believe it came from a trustworthy source, which is why spam and phishing campaigns regularly use these strategies.

- Spamming: Spam in the form of email, sometimes known as junk email, is a sort of spam. It's a mass email communication that hasn't been requested. Spam first became popular in the mid-1990s, and it is now an issue for the vast majority of email users. Receiver email addresses are collected by spambots, which are automated programs that scour the internet for email addresses. Spammers use spambots which then creates email distribution lists. In the hopes of receiving a few responses, a spammer will send an email to millions of email accounts.
- Cyber defamation: Cyber defamation is the harm done to a person's reputation in the eyes of others as a result of their use of the internet. Making a defamatory statement is intended to harm someone's reputation.
- IRC Crime (Internet Relay Chat): IRC servers allow people from all over the world to communicate with one another through a single platform, which is commonly referred to as a room. Cyber thieves primarily use it for meetings. Hackers use it to discuss their techniques.

2. Cyber Crime against property: Computer vandalism, intellectual property (Copyright, patented, trademark, etc.) property crimes, and so on are examples of these types of crimes.

   Intellectual property crime includes:

   - Software piracy: It is defined as the unlawful copying of software.
   - Copyright infringement: Violations of a person's or organization's copyright might be defined as plagiarism. It is the unauthorized use of copyright materials such as music, software, and text in simple terms.

3. Cyber Crime against organization:

Cyber Crimes against the organization are as follows:

- DOS attack: In this assault, the attacker floods servers, systems, or networks with traffic in an attempt to overwhelm the victim's resources and render them inaccessible or difficult to use.
- Email bombing: It's a sort of Internet abuse in which a large number of emails are sent to a single email address to overload or flood the mailbox or the server where the email address is hosted.
- Salami attack: Salami assault is also known as salami slicing. The attackers use an internet database to acquire customer information including bank account and credit card details in this attack. The attacker deducts very tiny amounts from each account over time. The hackers are undetected since the clients are unaware of the slicing, and there is no complaint made in this attack.

4. Cyber Crime against Society: Cyber Crime against society includes: Logical bombs, Trojan horses, Data diddling, and so on.
    - Forgery: Forgery is defined as the creation of a fraudulent document, signature, cash, or revenue stamp, among other things.
    - Web jacking: The term "web jacking" comes from the term "hijacking." When the victim clicks on a link on the attacker's fake website, a new page with the message appears, enticing them to click another link. If the victim clicks on the link that appears to be authentic, he will be taken to a fake page. These attacks are carried out to acquire access to or control over another's website. The attacker may also alter the contents of the victim's webpage.

Hacking and Data Theft

Sections 43 and 66 of the IT Act make it illegal to hack into a computer network, steal data, introduce and spread viruses through computer networks, damage computers, computer networks, or computer programs, disrupt any computer, computer system, or computer network, and deny authorized personnel access to a computer or computer network. The maximum penalty for the aforesaid offenses is 3 (three) years in prison or a fine of Rs. 5,00,000 (Rupees five lac), or both.

Because section 22 of the IPC states that the words "movable property" is intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything attached to the earth, section 378 of the IPC, which deals with "theft" of movable property, will apply to the theft of any data, online or otherwise. The maximum penalty is imprisonment of up to 3 (three) years or a fine or both.

It is possible to argue that the phrase "corporeal," which means "physical" or "material," excludes digital assets from the purview of section 378 of the IPC. The counter-argument is that the drafters wanted to safeguard all sorts of property, including land and anything permanently tied to the earth.

Receipt of stolen property

Dishonestly receiving any stolen computer resource or communication equipment is punishable under Section 66B of the IT Act. The individual receiving the stolen property must have done so dishonestly or had reason to realize it was stolen property, according to this provision. The penalty for this offense under Section 66B of the IT Act is up to 3 (three) years in prison or a fine up to Rs. 1,00,000 (Rupees one lac) or both.

Section 411 of the IPC, which is essentially equivalent to section 66B of the IT Act, also imposes penalties for dishonestly accepting stolen property. The penalty under section 411 of the IPC is either imprisonment of either kind for a period of up to 3 (three) years, or a fine, or both.

De Jure Nexus
LAW JOURNAL

Identity theft and cheating by personation

Identity theft and cheating by personation are punishable under Section 66C of the IT Act, which states that anyone who fraudulently or dishonestly makes use of another person's electronic signature, password, or other unique identification feature shall be punished with imprisonment of either description for a term that may extend to 3 (three) years, and shall also be fined which may be extended up to Rs. 1,00,000 (Rupees one lac).

Conclusion

In a digital era, it is indeed very hard to track and keep records of users and the information they surf regularly. Especially at a time when billions of users log onto the internet every day ranging from elementary school children to aged people. Hence it is very important to draft laws to keep the demography in mind. Even though there should be equality regarding laws, there must be

stricter and special provisions to apprehend minors and protect their interests. Children should have laws that safeguard their interests- protects them from getting influenced by unethical influences as well as ways to prevent them from getting exploited. They are the most vulnerable section as they believe anything they read on the internet and is the easiest target. As much as it is the responsibility of the parents, we must protect the future generation too.

We need stricter punishments when it comes to data theft. A person may be imprisoned for 3 years or fined up to 5 lacs. However, the damage done is irreparable. The government must first take measures to shut down the further distribution of data and punish the individual accordingly. The government must also look into mega corporates which get the consent of the user through a clickwrap or a browse wrap agreement where the user has no other choice. The company then feels entitled to commercialize the user's data. Customized and targeted ads are an example of this. The law must adequately punish these companies.

One of the major victims of non-consensual sharing of intimate images is women. Even after the perpetrator is caught, it takes a long time to process their requests and bring them to justice. The victim on the other hand suffers lifelong trauma and shame. Hence the Non-Consensual Sharing of Intimate Images Act 2021 must focus on the rehabilitation of the victim and be implemented accordingly.

De Jure Nexus
LAW JOURNAL