Available online @ www.iaraindia.com
RESEARCH EXPLORER-A Blind Review & Refereed Quarterly International Journal
ISSN: 2250-1940 (P) 2349-1647 (O)
Impact Factor: 3.655(CIF), 2.78(IRJIF), 2.77(NAAS)
Volume XIII, Issue 43
July- 2024
Formally UGC Approved Journal (63185), © Author

THE EVOLVING LANDSCAPE OF CYBER LAW AND CYBER SECURITY

SUMIYA FAROOK
III BA LLB (Hons.),
Crescent School of Law, Chennai, Tamil Nadu
&
MARIYAM MUBASSARA
III BA LLB (Hons.)
Crescent School of Law, Chennai, Tamil Nadu

Abstract

These days, people get everything they need on the internet. Anything that comes to mind may be done on the internet, including social networking and online learning. The internet and all its advantages increased the public's awareness of cybercrime. As individuals rely more and more on the internet, a wide range of cybercrimes have emerged. Cyber law comprises cyberspace, the internet, and any other topic related to information technology.

A robust ecosystem within a company is necessary to deter cybercrime. An ecosystem for an organization typically consists of three elements: automation, interoperability, and authentication. By creating a robust and secure system, the company would be able to defend these elements and fend off attacks from viruses, attrition, hackers, insider threats, and stolen equipment.

Key Words - Awareness, Advantages, Cyberspace, Cyber law, Information Technology

Introduction

A few years ago, there was a lack of knowledge about the crimes that may be committed online, but in terms of cybercrime, India is currently not far behind other nations where the incidence of occurrence is also rising. However, there are certain risks associated with computers and the internet that might negatively affect civilizations. Cybercrime poses a threat to many individuals and entities that have computers linked to the internet, especially those using mobile devices. Governmental organizations, as well as private citizens, rely on information technologies for most of the information processing in the current environment. It is impossible to overstate the importance of government and commercial enterprises hiring and retaining highly skilled cybercrime experts. For the Organization to succeed, cyber activity control, prevention, and investigation are essential.

Online crimes are often broadly classified into three primary groups, including: 1.Individual 2. Property 3.Administration 4. Individual

Cyber stalking, trafficking, distribution, and "grooming" are examples of this kind of cybercrime. Law enforcement organizations currently take cybercrime extremely seriously and are cooperating globally to track down and apprehend those responsible.

2. **Property**

In this scenario, cyber offender embezzle money by stealing bank account information, use credit card fraud to make regular online purchases, con unsuspecting people out of their hard-earned cash, or use malicious software to break into an organization's website or interfere with its operations. Just as vandals harm property offline, bad malware may likewise harm hardware and software.

3. **Government**

Cyber terrorism is the name given to crimes committed against a government. If criminals are successful, the public may become terrified and devastated. This type of criminal propagates propaganda or hacks military or government websites. Terrorist organizations or hostile foreign governments may be the perpetrators**.**

Background

In 1820, the first cybercrime was documented. Although the first computers appeared in Japan, China, and India about 3500 B.C., Charles Babbage's analytical engine is regarded as the invention of the modern computer. The loom was invented in France in 1820 by Joseph-Marie Jacquard, a textile maker. This gadget made it possible to weave unique textiles or materials using a continuous sequence of stages. As a result, the workers at Jacquard became extremely concerned about their lives and conventional jobs, and they chose to sabotage to dissuade Jacquard and prevent them from using the new technology in the future.

Cyber Law

The creation of Cyber Law aimed to regulate crimes carried out using computer resources, the internet, or cyberspace. Cyber Law is the term used to describe the legal concerns pertaining to the usage of computers or communication technologies. The goal of creating Cyber Law was to control crimes committed using computers, the internet, or cyberspace. The phrase "cyber law" refers to the legal issues surrounding the use of computers and other communication technology.

- It is advisable to carefully examine the internet legislation.
- a basic understanding of the Internet and its security.
- Read about incidents of cybercrime. One might become aware of such crimes by reading those cases.
- The effect of technology on crime. The 2000 Indian Information Technology Act the Information Technology Act, 2000 (ITA-2000, or the IT Act) is an act of the Indian Parliament (no. 21 of 2000), as stated in Wikipedia. It was notified on October 17, 2000. The most

significant legislation in India pertaining to electronic trade and digital crimes, or cybercrimes, is this one. The United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model), which was suggested by the UN General Assembly in a resolution dated January 30, 1997, serves as its foundation. The following are some of the main ideas of the Information Technology (IT) Act of 2000:

- Nowadays, email is regarded as a legitimate and authorized means of communication.
- Act has opened new economic opportunities for organizations to become the Certifying Authorities and issue digital certificates.
- The primary purpose of this Act is to address the security issue. It established the concept of digital signatures, which are used to confirm an individual's identity online.
- The Act offers the corporation financial compensation as a remedy if criminals cause the organization any injury or loss. India's Cyber Law The sections under the IT Act of 2000 are listed below.

1. **Section 66- Computer** system hacking, data manipulation, etc.

Whoever intends to cause harm, loss, or to erase, change, or destroy any information stored on a public computer system or on the computer of an individual. Hacking is any action that reduces its usefulness, devalues it, or negatively impacts it in any way.

2. **Section 66A-** Using any kind of communication facility to send abusive remarks. Any message or information that is offensive or contains threatening language sent through any communication service; • Any information that is false or invalid and sent with the intent to cause annoyance, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred, or ill will.

3. Any email or electronic communication sent with the intention of upsetting, upsetting, or misleading the recipient about where the message originated. Penalties: Anyone found guilty of offences covered by this section faces a maximum penalty of three years in jail and a fine.

3. Section 66B

Acquiring communication equipment or computer resources that have been stolen Insincere willfully accepting or holding onto any stolen computer, computer resources, or communication devices, or having reasonable suspicion that one is doing so.

4. Section 66C

Theft of identity, the unauthorized use of a password, digital or electronic signature, or any other form of unique personal identity is illegal. Penalties: An individual found guilty of these offences may face a maximum sentence of three years in jail and a fine of one lakh rupees.

5. Section 66D personating someone while using a computer to cheat Anybody who attempts to deceive another person by using a computer or communication equipment to impersonate someone else would be punished with a fine of up to Rs. 1 lakh and/or a period of imprisonment lasting up to three years.

6. **Section 66E**

Security infringement or breach? Anybody found to have intentionally or knowingly published, transmitted, or taken pictures of another person's intimate areas without that person's consent and violating their right to privacy faces a maximum sentence of three years in prison, a fine of two lakh rupees, or both.

7. **Section 66F**

- Terrorism using the internet A. Anybody who knowingly threatens the security, integrity, unity, or sovereignty of the people or any group of people or incites panic among them I. Denies anybody access to computer resources.
- Attempting to breach security or get unauthorized access to a computer resource or to use more access than is permitted.
- introducing any computer contaminant, and by doing so, causes or is likely to cause death, injury, or destruction of property; or disrupts, or it is likely to cause, the supply or services that are necessary for people to survive; or adversely affects the infrastructure of critical information as defined by section 70 of the IT Act.
- Penalties: Life in prison is the penalty for anybody who plans or carries out such cybercrimes or cyberterrorism.

8. **Section 67** - sending or disseminating pornographic content online Anyone who uses electronics to transmit, publish, or induce to disseminate any pornographic content. Anything that is vulgar, lubricious-seeming, or if it tends to corrupt anyone who is likely to consider all relevant circumstances when reading, seeing, or hearing the matter that is contained in it, shall be sentenced on the first convict with either description for a term that may extend up to five years of imprisonment along with a fine that may extend up to one lakh rupees. On the second or subsequent convict, it may be sentenced with either description for a term that may extend up to ten years of imprisonment along with a fine that may possibly reach two lakh rupees.

Positive and Negative Aspects of the It Act

- The existence of this Act has allowed many businesses to undertake e-commerce without worry. Up until recently, the absence of a legislative framework to regulate internet business transactions hampered the growth of electronic commerce in our nation.
- Furthermore, the Act makes it possible for business organizations to serve as Certification Authorities in connection with the Act's issuing of Digital Signature Certificates. If the government's requirements are met, there are no restrictions under the Act regarding the type of legal body that can be recognized as a Certifying Authority.
- Additionally, it offers details on security issues that are vital to the effectiveness of using electronic transactions. The phrase "secure digital signatures" was established and accepted as part of the Act; these signatures must have been subjected to a set of security procedures.

It follows that digital signatures are now safe and will be very important to the economy. Securing online transactions can be facilitated with digital signatures.

- The Act allows the firms to use the electronic form established by the relevant government to electronically submit any of their papers with any office, authority, body, or agency that is owned or managed by that government.

Indian Penal Code, 1860(IPC)

- **Section 292:** Originally intended to deal with the selling of pornographic materials, this section has expanded to include a variety of cybercrimes in the digital era. This clause also governs how pornographic content or child-exposed sexual activities or exploits are published or communicated via technological means. Such activities are punishable by up to two years in jail and a fine of Rs. 2000, respectively. Any of the offences carry a maximum sentence of five years in jail and, for repeat (second time) offenders, a fine of up to Rs. 5000**.**
- **Section 354C:** Under this clause, capturing or disseminating images of a woman's intimate areas or behaviour without her permission is considered cybercrime. Since it entails witnessing a woman engage in sexual activity while under the legal age, voyeurism is the only topic covered in this section. Both Section 66E of the IT Act and Section 292 of the IPC are sufficiently wide to cover acts of a similar kind in the absence of the necessary components of this section. First-time offenders may be sentenced to up to three years in prison, while repeat offenders may be sentenced to up to seven years, depending on the nature of the offence.
- **Section 354D**: This chapter describes and penalizes stalking, including physical and cyberstalking. Cyberstalking is the tracking of a woman by email, the internet, or other technological methods, or the attempt to get in touch with her despite her lack of interest.

  For first-time offenders, the maximum sentence is three years in jail; for repeat offenders, it is five years, plus a fine.
- **Section 379**: Theft is punishable by up to three years in prison in addition to a fine under this section. The fact that many cybercrimes involve stolen computers, stolen data, or hijacked electronic devices is one reason why the IPC Section is relevant.
- **Section 420**: This section addresses dishonestly inducing the handover of property and cheating. This clause imposes a fine and a seven-year jail sentence on cybercriminals who commit offences such as building bogus websites and cyberfraud. Crimes pertaining to creating fake websites or stealing passwords for fraudulent purposes are covered under this provision of the IPC.
- **Section 463**: Electronic document or record falsification is covered under this section. Under this clause, spoofing emails carries a maximum sentence of seven years in jail and/or a fine.
- **Section 465**: The penalties for forgeries are usually covered by this section. Under this provision, acts including forging electronic mail addresses and creating fraudulent papers online are dealt with and penalized by up to two years in jail, or both.

- **Section 468**: A seven-year jail term and a fine are imposed for fraud committed with the purpose to deceive. Email spoofing is also penalized in this area.

Safety in Cyberspace

Use a strong password whenever feasible, and if you use webmail, activate two-step authentication. Setting up security for your social media or webmail accounts is crucial. Strong password guidelines:

A password should include at least eight characters.

It is recommended to include one or more lowercase, uppercase, numbers, and symbols.

- Never communicate or exchange any private information, including passwords, bank account numbers, and ATM pins, over unencrypted mail or via an unencrypted connection. Unencrypted websites are those that lack the lock symbol and https in the browser's address bar. The website is secure because of the "s," which stands for secure.
- Don't register on any social networking site until you are of legal age.
- We refer to this as a drive-by download. Pop-ups that offer site surveys or anything similar on e-commerce sites should be ignored since they can be malicious programming.

Types of cyber crime:

Hacking:

A person's computer is compromised to get sensitive or private data. Hacking is classified as a crime and subject to punishment in the US. This is not the same as ethical hacking, which is a technique used by many companies to assess the security of their online presence. When someone hacks into someone else's computer, they may not be aware that their computer is being accessed remotely and that they are using a variety of applications to do it. Password cracking software is another tool that many crackers use to attempt to obtain access to resources. Hackers could load data onto users' computers and keep an eye on what they do there. Unbeknownst to them, a hacker may install many programs on their PC.

Theft

When someone downloads software, games, movies, music, or other content in violation of copyright, it is considered this kind of cybercrime. Even peer-sharing websites promote software piracy, and the FBI is currently focusing on a number of these websites. These days, the legal system deals with cybercrime and regulations are in place to prevent people from downloading illegally.

Malicious software:

This malware, which is often known as a computer virus, is Internet-based software or programmed, designed to cause network disruptions. The program is used to break into a system and obtain private data or information, or it can be used to harm other software that is already installed in the system.

Identity theft

This is a significant issue for anyone who uses the Internet for banking and monetary transactions. In this type of cybercrime, an offender obtains access to a victim's bank account, credit cards, debit card, Social Security number, complete name, and other private information to embezzle funds or make purchases online using the victim's identity. The information that a person provides to an identity thief can be used to file taxes, seek credit, or obtain medical care. The victim may suffer significant financial losses as a result, and their credit history may even be damaged.

Computer vandalism:

This kind of cybercrime doesn't include theft; instead, it involves damaging or destroying data. It spreads viruses. Cyber terrorism is the use of online assaults for terrorist purposes. Terrorists with an understanding of technology are employing 512-bit encryption, which cannot be cracked.

Online job Fraud:

An online job fraud plan is deceiving job seekers by offering them false hope and a better position with a bigger salary.

Phishing:

Phishing fraud occurs when an email purports to be from a reliable source but really contains a malicious attachment used to steal user personal data, including ID, IPIN, card number, expiration date, CVV, and so on. The data is then sold on the dark web.

Vishing

Vishing involves utilizing victims' phones to steal sensitive information. Cybercriminals coerce victims into disclosing personal information and granting access to personal accounts by employing sophisticated social engineering techniques. Like phishing and smishing, vishing deceives victims into believing that answering the call is a sign of politeness. It is common for callers to pose as representatives of the government, tax agency, police department, or victim's bank.

Smishing

Smishing, as the name implies, is a scam wherein victims are tricked into contacting a fictitious number, accessing a fraudulent website, or installing dangerous software that remains on their computer using text messages sent via mobile phones.

Credit card Fraud

Unauthorized transactions or card withdrawals are committed in credit card (or debit card) fraud to get the victim's money. Credit/debit card fraud occurs when money is taken out of a customer's account without authorization or when unauthorized purchases are made. When a criminal obtains knowledge of a cardholder's personal identification number (PIN) or debit/credit number, fraudulent conduct takes place. Your data may be accessed by dishonest workers or cybercriminals.

Differences between Cyber Crime and Cyber Security

Cyber security is more than just following rules and taking precautions against online fraud. Cyber security’s goal is to make it more difficult for hackers to identify and take advantage of weaknesses in business and governmental networks. In contrast to conventional crime, cybercrime often prioritizes protecting the privacy of individuals and their families when they participate in online activities.

1. Crime types: Cybersecurity crimes are those in which, should they become hacked, a computer programmer, piece of hardware, or computer network becomes the primary target of an attack. However, the primary objectives of cybercrime are a particular individual or group of people as well as their data.

2. Victims: Secondly, the kinds of victims in these two professions also differ from one another. In cyber security, the main targets are governments and companies; in cybercrime, victims might include people, families, organizations, governments, and corporations.

3. Subject matter: Scholars in two distinct disciplines study these two subjects. Cyber security is a subfield of information technology, computer science, and computer engineering. To improve network security, engineering, networking, and code development are utilized. Cybercrime, on the other hand, is classified as social, psychological, and criminological. It alludes to a hypothesis on why crime happens and how to stop it.

Cyber Security Strategies • Ecosystem

• E-Goverance

Through e-governance, the government can offer services online. However, many nations do not use e-governance to its potential. The goal of cyberlaw should be to advance this technology so that citizens have more control.

• Open Standards

Open standards directly lead to improved security against cybercrime. Open standards make it simple for both people and enterprises to put in place the right security safeguards. Additionally, a wider choice of new technologies and a higher rate of economic growth will be made possible by these standards.

• IT Mechanisms

There are several useful IT tools or methods at one's disposal. Promoting these controls and methods is crucial to the battle against cybercrime. Among the measures are data encryption, association-based protection, link-based protection, and end-to-end protection.

Need For Cyber Laws In India

Cyberlaw is especially important in nations like India where internet usage is commonplace. The law was passed to defend people and organizations against cybercrime. If someone infringes and breaks the law, other persons or organizations may be able to take them to court under cyberlaw-

- Since all stock transactions are now completed in demat format, everybody participating in these transactions is covered by cyber law if any fraudulent transactions occur.
- Technology is advancing so quickly that people are filling out government papers online, including income tax returns and service tax reports. Because anybody may abuse those forms by breaking into official websites, cyberlaw is necessary to pursue legal action.
- Electronic contracts and digital signatures are commonly used in business transactions. Anyone working with digital signatures and electronic contracts can simply abuse them. Cyberlaw offers defense against these kinds of frauds.

Impact of Cyber Crimes

- **Leakage of Personal Information**

People suffer from more than simply monetary losses when their personal information is compromised. Despite its safety, many social networking sites still provide an open platform for anybody to view the lives of others, which can be harmful. In addition, hackers can access user accounts and obtain any data they choose. People are harmed by phishing and spamming as well.

- **The Treat to National Security**

Customers begin to lose faith in these websites and applications because of these monetary losses and the risk to their personal information. The website or software is deemed dangerous and deceptive, even if someone else is a criminal. Furthermore, it discourages customers from initiating a purchase when their credit card information is requested. This undermines an e-enterprise's credibility, endangering a possible business.

Conclusion

Cyber laws need to be updated and improved constantly to keep up with the growing dependency of humans on technology, both in India and throughout the world. The epidemic has also resulted in a notable rise in the number of remote workers, which has raised the demand for application security. Legislators must take additional care to stay ahead of imposters so they can act against them as soon as they appear. It can be prevented if lawmakers, internet providers, banks, shopping websites and other intercessors work together. However, ultimately, it is up to the users to participate in the fight against cybercrime. The only way for the growth of online safety and resilience to take place is through the consideration of the actions of these stakeholders, ensuring they stay within the confines of the law of cyberspace.

The IT Act, 2000 was passed by the Indian government to combat cybercrimes. The Act also amends the Reserve Bank of India Act of 1934, the Banker's Books Evidence Act of 1891, the Indian Evidence Act (IEA) of 1872, and the Indian Penal Code of 1860. Cybercrime may begin anywhere on the globe and spread across national borders via the internet, making it more difficult to investigate and prosecute these crimes legally and technically. To combat cybercrimes, international harmonization efforts, coordination, and cooperation among many states are essential. Our primary goal in producing this essay is to educate the public about cybercrime.

Reference

1. Rai, D. (2021, September 15). *Cyber Crime and Cyber Law: An overview of* iPleaders. https://blog.ipleaders.in/introduction-to-cyber-crime-and-cyber-law/
2. Agarwal, H. (2023, August 16). *Everything about Cyber Laws in India | App Knox*. Appknox. https://www.appknox.com/blog/cybersecurity-laws-in-india
3. Patil, J. (2022, March 3). *Cyber Laws in India: An Overview*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4049059