International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 12-11-2021, Accepted: 26-11-2021, Published: 13-12-2021
Volume 3, Issue 4, 2021, Page No. 54-56

"Cyber crime and cyber law in India: An in-depth overview

Sudipta Ranjan Sahoo
Department of Law, Mats University State, Raipur, Chattisgarh, India

Abstract
The internet's function and use is growing quickly over the world. It has made life easier for consumers, but it has also made it easier for hackers to access whatever data and information that individuals consciously and unwittingly provide on the internet and elsewhere. People need to be made aware and taught about cybercrimes in addition to adequate regulations to protect and prevent cybercrimes. So let's get some in-depth overview of Cyber Crime and Cyber Law in India.

Keywords: cyber crime, cyber law in India, why cyber law in India, sudipta ranjan sahoo

Introduction

Everyday life has become more and more reliant on the internet. Everyday activities, like as purchasing food online, researching a topic, looking at memes, and writing online about your whereabouts, have become so engrained in our lives that we tend to overlook the dangers and risks they provide. Because the internet is a worldwide platform, it is available to anybody. Individuals begin breaking things as soon as they have access to them. Cyberspace is referred to as the Internet because of the worldwide computer network that makes it possible to communicate online. This platform allows for user-to-user conversation for the sharing and exchange of ideas and information. If you want to put it another way, Cyberspace refers to this computer-generated global stage for the internet and the web. Under Indian law, the term "cybercrime" is not defined. All of India's laws pertaining to information technology are silent on the subject of the Information Technology Amendment Act of 2008. Even after the Information Technology (Amendment) Act, 2008, the Indian Penal Code does not include the term "cybercrime" in its definitions. For example, cybercrime may be defined as an unauthorized access into another computer system or database; manipulation of data; hacking; spam; cyber-warfare; and the transmission of computer viruses. A computer-aided crime or offence is defined as such in this example.

On the subject of Cyber Law, it is described as a system of rules that govern Cyberspace, protect citizens from cyber crimes, and impose penalties on those who break them. According to this definition, "cyberlaw" refers to both legal authority and control over various sections of the internet and computer security. India's cyber regulations are governed under the Information Technology Act, 2000. –

Impact of Cyber Crimes in India

Impact on Indian Economy

Many people now use computers or the internet to transfer money or pay bills, and this trend is expected to continue. There is a high likelihood that you may become the victim of an online money scam as a result. It has been estimated that 74 million American citizens have been victims of cybercrime, which has cost the country an estimated $32 billion. When it comes to online transactions in India, where "cashless India" has become increasingly popular, there are greater dangers of being tricked if one is not attentive enough to utilize safe online platforms and apps. More than 80 percent of the firms polled admitted that cybercrime had resulted in losses.

Leakage of Personal Information

In addition to financial losses, people are also harmed by illegal access to their personal data. Many social networking sites, no matter how safe, are still open platforms for anybody to monitor someone else's life, and this can be dangerous.In addition, hackers can get access to a user's account and steal any information they choose. They also inflict harm to others via spamming and phishing

Loss of Consumer Trust

Consumers begin to lose faith in these sites and applications when they lose money and their personal information is at risk. It does not matter who the culprit is; the site or app is still regarded as fraudulent and hazardous, regardless of who is responsible for it. Since credit card information is sought, many clients are put off by the prospect of making a transaction. E-credibility, an enterprise's, and prospective customers are all negatively impacted by this.

The threat to National Security

Computers and networks are increasingly being used in the military of most countries today. Malware, which may cause network outages and propagate disinformation, can be spread via information warfare, which is a relatively new phenomenon. Even terrorists and hackers are using these technologies to infiltrate foreign security networks and steal information. Threats and warnings can also be sent using computer systems.

Need of Cyber Law in India

The number of cybercrime cases has increased as the internet, information technology, and computers have developed. As a

consequence, cyber laws include every area of law where cybercrimes might be committed, including criminal law, contract law, intellectual property law, and tort law. Besides free speech, safety, intellectual property, privacy and terrorism, cyber laws also deal with jurisdictional issues related to cyber laws.

With an ever-increasing number of people using the internet, it has never been more important to have and enforce effective cyber laws. As a result of the following:

1. As payment applications and websites have become more popular, consumers are increasingly turning to online transactions because they are convenient and time-saving. Additionally, the government's "Cashless India" programme has seen an increase in the number of online transactions.
2. When it comes to interacting with each other, email, SMS, messaging apps, and social networking sites have taken over.
3. The security of an organization's electronic data is heavily reliant on the computer networks that support it.
4. The majority of government forms, such as Income Tax Return, Passport application, Pan Card application, Company legal forms, etc., are now filled out electronically.
5. Transactions may now be completed in a matter of seconds thanks to the use of digital signatures and authorization.
6. Using computers and networks to commit non-cyber crimes is also aided by this technology. Computers and mobile phones now hold the vast majority of our personal information. For example, evidence gathered from kidnapping, terrorist attacks, counterfeit currency, and tax fraud can be used to prosecute criminals.
7. Laws governing cyberspace are essential to establishing and defining a model of cyber society and ensuring the protection of cyber property.
8. There has been an increase in the use of digital contracts in the modern era, and these contracts are protected by cyber laws.

Scope of Cyber Law in India

Since the internet and computer technology provide a wide range of difficulties and risks, cyber law covers a wide range of issues and concerns:

1. “Dealing with computer hackers,, spammers, and those who disseminate malware and viruses.
2. Privacy for people and combating money transactions scams.
3. Regulations and classification of contractual duties connected to software procurement.
4. Protecting intellectual property rights and addressing concerns of copyright in a computer programme and patent protection of software programmes.
5. Dealing with purchases from other countries under e-commerce rules and regulations.
6. dealing with the issue of domain name trafficking within the legislation
7. Regulation of online content and information is necessary.
8. Rights to free speech and access to information are regulated.

Cyber Law in India and the IT Act, 2000”

The Information Technology Act, 2000, provides the framework for Indian cyber regulations (IT Act). E-commerce and electronic forms, as well as the expeditious filing of electronic records with the Government, are the key objectives of this Act. Cybercrime, electronic information, electronic authentication and digital signatures, and the responsibility of network service providers are all addressed in this legislation. The I.T. Act is based on the United Nations Model Law on Electronic Commerce 1996, which was approved by the United Nations General Assembly (UNCITRAL Model).

These are the primary topics of cyberspace and cybercrime that are covered under Indian Cyber Law:

1. This implies that whatever you create, distribute, or publish in electronic form is now permissible under the Indian Cyber Law.
2. All electronic contracts are now lawful under the new law, which implies that an electronic contract may be established by making an offer and accepting it electronically.
3. Under the Indian Cyber Law, digital signatures and electronic authentications are permitted.
4. The Indian Cyber Law encompasses a wide range of cybercrimes and imposes penalties on those who commit them.
5. As long as the crime is committed on a computer or network located in India, it also punishes foreigners.
6. All electronic publications, chats, signatures and authorizations are now legally legitimate and may be used in any judicial processes as a result of the legalisation of electronic media.

Pros of the I.T. Act, 2000

1. I.T. Act, 2000, recognized email and text message exchanges as ordinary forms of electronic communication and legalized their use as evidence in court. Following the adoption of the Information and Communications Technology Act of 2000, electronic forms and communications became legal, and they may now be used in court as evidence.
2. Now that the IT Act, 2000 has been passed, businesses may engage in e-commerce and e-business and promote online transactions economically.
3. Online transactions have benefited greatly from the I.T. Act, 2000, which allows for the use of digital signatures and authentications, which authenticates an individual's identity on the internet.
4. A corporation's computer systems and networks may be breached by anybody, and the 2000 I.T. Act provides for statutory damages if that person causes any harm. An further type of punishment for such activities is provided under the I.T. Act, 2000, which includes monetary penalties.
5. A number of cyber crimes have been defined and punished under the I.T. Act, 2000. These include hacking, spamming, identity theft, and phishing, all of which are criminalised under the act. There was no legal remedy for cybercrimes prior to the passage of this Act, since they were not included in any legislation.
6. Certifying authorities are corporations that can issue digital certificates under the authority of the Act.
7. This legislation also permits the government to issue notifications over the internet via e-governance.

“Cons of the I.T. Act, 2000

1. The I.T. Act, 2000 may cause a conflict of jurisdiction.
2. The domain name system is the foundation of electronic business. I.T. Act, 2000 does not deal with domain names,

the rights and obligations of domain owners, nor does it deal with the subject of domain name transfers.
3. Despite the prevalence of copyright and patent concerns in respect to computer programmes and networks, the I.T. Act, 2000 does not safeguard intellectual property rights.
4. The I.T. Act, 2000 does not specify or cover all offences that may be committed in relation to information technology. Computer programmes and networks are always evolving, thus the nature of cybercrime is also altering with the growth of technology. Cyberstalking, cyber fraud, chat room abuse, theft of internet time, and many other types of cybercrimes are not covered by this legislation.
5. It is imperative that the I.T. Act, 2000, address concerns like privacy and content control, given the dangers posed by the internet.
6. Third and most important is that of the Act's implementation. The I.T. Act, 2000, does not provide any criteria for its implementation or restrictions.

Information Technology (Amendment) Act, 2008"

The I.T. Act, 2000, has undergone a few changes since its inception, which have enhanced some of its aspects. The following are some of the amendments:

1. It has been changed to "electronic signature" to make the Act more technology-neutral.
2. There is now a clear definition of the word "Communication device" Any device that is used to communicate, convey, or transmit any type of media is referred to as a "commuication device," which includes mobile phones and personal digital assistants (PDAs).
3. "It has also been defined as a facility from which internet access is made available to the general public in the course of business by any individual or group.
4. Sections have been added to handle data protection and privacy."

Conclusion

The internet's function and use is growing quickly over the world. It has made life easier for consumers, but it has also made it easier for hackers to access whatever data and information that individuals consciously and unwittingly provide on the internet and elsewhere. People need to be made aware and taught about cybercrimes in addition to adequate regulations to protect and prevent cybercrimes.

However, despite the fact that internet users can freely share their personal information, The state has a responsibility to protect its people' interests. Large organizations, such as Facebook, have lately been revealed to utilize the personal information and data of its users to sway people's political opinions. Individuals' privacy is imperiled, and the interests of the United States are imperilled as well. The I.T. Act, 2000, skillfully solved the issue of cybercrime in India, however the Act's efficient implementation is still lacking.In light of the current situation, effective cyber regulations are clearly needed, but individuals should also be aware of the dangers they face while accessing the web.

References

1. https://www.southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf
2. https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf
3. https://www.bbau.ac.in/dept/Law/TM/1.pdf
4. http://osou.ac.in/eresources/introduction-to-indian-cyber-law.pdf
5. https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence