A UNIT OF
LAW LABORATORY

MAY 2022

Law Laboratory Research Journal of Law & Socio-Economic Issues

ISSN: 2583-0783

VOLUME 1 | ISSUE 3

WWW.LAWLABJOURNAL.IN

A STUDY ON EMERGING ISSUES IN CYBER LAW

- *Anjali Lakhwani*[1]

ABSTRACT

All that in this day and age is racing to the digital world, utilizing digitization and systems administration to accelerate their admittance to the web-based world's abundance of advantages. Showcasing, trade, and correspondence have all been altered, and new, beforehand non-existent areas like internet advertising, web-based business, and online interchanges have all arisen. Notwithstanding, just like with advancement, the hunter develops soon after the prey. Subsequently, the web-based world brought forth a totally new sort of criminal procedure known as digital wrongdoing. To manage the appalling wrongdoing of cybercrime, building the rule of law simultaneously is basic.

One potentially negative side-effect of quick industrialization and digitization is the rise of the internet. The internet immensely affects essentially every part of life and the economy, yet it has likewise brought forth another crime worldview known as digital wrongdoing. To stay aware of the legitimate part of this situation, Cyber Law was made. The web was initially created for military correspondence and insight, yet it has since developed into a tremendous organization that includes everything possible.

Keywords: Cyber Law, Cyber Crime, Cyber Security, Cyber Ethics, System Intrusion, Cybernetics

INTRODUCTION

The advancement of technology has resulted in the creation of a cyber world, or cyber space. With the fast progress of information technology, cyberspace is undergoing significant transformation.

To take advantage of the tremendous benefits of the online world, everything in today's world is racing to the cyber world via digitization and networking. Marketing, commerce, and

[1] 4th Year, B.B.A. LL.B., Amity University, Chhatisgarh

communication have all been revolutionized, and new, previously unknown industries have evolved, such as online marketing, e-commerce, and online communications. The predator, however, evolves quickly after the prey, as is typical in evolution. As a result, cybercrime emerged as a brand-new form of criminal strategy. To cope with the tragedy of cybercrime, it is important to simultaneously create law and order.

The upshot of the globalization of technical ecosystems has produced a two-edged sword with a significant good and a significant bad side. The emergence of cyberspace is an unintended consequence of fast progress and digitalization. Cyberspace has had a huge impact on practically every aspect of life and business, but it has also given rise to a new type of criminal behaviour known as cybercrime. The internet was created to facilitate military communication and intelligence gathering, but it has now evolved into a massive network that encompasses virtually everything. Cyber Law was created to stay up with the legal aspects of this situation.

In July 2013, the Indian Government established a plan for national cyber security in response to a cyberattack that attacked the government's official email. However, this regulation does not appear to have solved all the problems associated with cybercrime. Because the policy merely provides instructions for normal operating procedure, it does not optimise the potential for maximum advantage.

LITERATURE SURVEY

As technology advances, so do illegal activities, and the IT Act of 2000 establishes procedures for dealing with cybercrime. In terms of electronic commerce, this technique offers certain advantages, but it does not solve all of the problems and challenges immediately.[2]

The IT Act is seen as an ambiguous regulation since the internet's jurisdiction is unclear. In the realm of cybercrime evidence investigation, computer forensics is becoming increasingly important because, while Although evidence is palpable in the physical world, erasing data from a computer system in cyberspace is tough. Because each error results in evidence disappearing, computer forensics necessitates the assistance of a capable and efficient computer specialist.[3]

Even though the IT (Amendment) Act 2008 addresses new issues, the IPC does not utilise the word "cybercrime" at any time. After 2008, there was a rise in cybercrime as criminals

[2] Maneesh Taneja and Dr. D.B Tiwari, *Cyber Law*, International Referred Research Journal, vol.11 (21) October, 2010, pp. 63-65

[3] Yougal Joshi and Ananda Singh, *A Study of Cyber Crime and Security Scenario*, International Journal of Engineering and Management Research, vol.3 (3) June, 2013, pp.13-18

discovered gaps in the law and used them to carry out illicit acts. Cybercrime may target people, the government and property.[4]

There aren't many legal precedents for reference and prior legislation were insufficient to deal with the offence at hand. Cyber laws must be strengthened. Our system should include harsh penalties as a deterrence to future illegal behavior.[5]

E-courts, online dispute resolution functions, effective cyber legislation, cyber forensics, and other aspects of India's development have not been realized. The IT Act need reform. In addition, lawyers in India should receive scientific and technological professional training.[6]

Given the geographical indeterminacy of the internet, one of the newest forms of crime is cybercrime, it also has the potential to cause havoc with every aspect of existence since this kind of crime is simple to conduct yet extremely difficult to identify and find in terms of jurisdiction.[7]

An enemy is a person who does something harmful. Outsider and insider adversaries both exist. Insiders and outsiders are not the same thing. An insider is a person who has been granted access to a nuclear power plant or other sensitive activities. Their authority, such as the ability to get admission, complemented them. Cybercrime is a multibillion-dollar problem, and there is a need to implement appropriate laws to protect the benefits of the computer era from being squandered.[8]

WHAT ARE THE AREAS OF DEVELOPMENT OF CYBER LAW IN INDIA?

The United Nations Commission on International Trade Law, often known as UNCITRAL, was established in 1996 by the United Nations, took the first move toward developing cyber rules in the twentieth century. It was acknowledged there that users, criminal and deterrent enforcement agencies should all be the emphasis of legal laws, because the individual who misuses technology, not the technology itself, bears responsibility for the crime. This went on to prove, for the first time, the importance of understanding that the crime is committed by humans, not by computers or technology. Following that, the United Nations General Assembly recommended

[4] Ravikumar S. Patel and Dr.Dhaval Kathiriya, "Evolution of Cybercrimes in India" International Journal of Emerging Trends & Technology in Computer Science, vol.2 (4) July – August 2013.

[5] Talwant Singh, *Cyber Law and IT*, pp. 1-4

[6] Prabhat Dalei and Tannya Brahme, *Cyber Crime and Cyber law in India: An Analysis*, International Journal of humanities and Applied science, Vol.2 (4), 2014.

[7] Aashish Kumar Purohit, *Role of Metadata in Cyber Forensic and Status of Indian Cyber Law*, International Journal of computer technology application, vol.2(5) sepoct, 2011.

[8] Angshuman Jana and Kunal Kumar Mondal, *A survey of India Cyber Crime and Law and its prevention approach*, International Journal of Advance Computer Technology

that each state consult the UNCITRAL Model Law while drafting cyber laws. The Indian government recognized the necessity to legislate in accordance with the UNCITRAL Model Law, as recommended by the UN General Assembly. As a result, the IT Act of 2000 was drafted and implemented. The Indian Penal Code was amended as a result of the adoption of the IT Act 200. Major developments were recognized, including the acknowledgement of electronic evidence and the management of electronic records and documents. Only tangible evidence and paperwork had legal standing before. In summary, the legislation covers the following topics:

1. Electronic document legal identification.
2. Digital Signatures' Legal Identification
3. Justice for Offenses and Violations
4. Cybercrime Dispensation Systems

The IT Act of 2000 tries to meet the requirements of the cyber era's legal system, as well as dealing with cybercrime in the context of the country's limited e-commerce potential. It makes a bold attempt to establish an infrastructure that enables e-commerce by providing legal underpinnings such as electronic signature recognition. However, the Act does not exempt uncertainty in certain areas, such as internet jurisdiction. Section 1 (2) states that the act applies to all of India, as well as any office or violation thereof conducted outside of India by any person.

WHAT ARE THE EMERGING ISSUES IN CYBER LAW?

With the rising use of digital technology, cyber law is expected to face a variety of new developments. The various issues include -

a) *Mobile law problems* - The increased use of mobile devices has extended the mobile ecosystem, and the resulting content is expected to pose significant challenges to cyber legal precedents from around the world.

   There are no specific restrictions governing the usage of these new mobile platforms and communication devices in several nations throughout the world, even though the usage of input and output through mobile devices is increasing every day.

   With the surge in mobile crimes, it's more vital than ever to address the legal concerns that come from mobile device use and to ensure mobile privacy and security.

b) *Concerns relating to cyber security* - Another emerging cyber law subject is the need for appropriate legal frameworks for preserving, promoting, and growing cyber security.

Cyber security incidents and network assaults are on the rise, culminating in breach of cyber security that might have significant consequences. However, a legislator's job is to not only create appropriate legal frameworks for protecting and preserving cyber security, as well as instilling a cyber safety habit among internet users.

c) *Cloud computing & Law -* With the advancement of internet technology, cloud computing is becoming more popular. Cloud computing presents new issues to legislators.

Data security, jurisdiction, data privacy, and other legal issues might be among the particular challenges. Stakeholders and cyber policymakers will under pressure to produce an acceptable legislative framework that benefits the industry and provides significant remedies in the event of cloud computing disasters.

d) *Social Media & Legal problems -* A recent study claims that social networking sites are too responsible for a slew of problems. Since law enforcement and intelligence organizations have been focusing on social networking sites, they have become the ideal storehouse for all data.

Crimes such as cyber harassment, cyber stalking, and identity theft have all been linked to inappropriate social media usage. Regardless of the efforts of many parties, social media users' privacy will be seriously undermined. The number of lawsuits involving social media content is expected to increase. Defamation and matrimonial lawsuits are becoming more common, thanks to the data and information saved on social media networking sites, there is a growing trend of other types of lawsuits in the future years.

e) *Laws on Spam -* Spam is becoming more prevalent in both email and mobile devices. Many nations have already established themselves as spam hubs. As the number of mobile users and internet expands, spammers are employing novel strategies to target digital customers. Because of these strong legal measures are essential to prevent the menace of spam.

OBJECTIVE OF THIS RESEARCH

The objectives of this research are -

a) *Create Awareness -* Because there is no national regulatory framework for cybersecurity, there is a knowledge gap at both the business and individual levels. Domestic citizens can only be safeguarded and protected from cyber-attacks if legislation is directed and managed.

The United States Government has designated October as National Cybersecurity Awareness Month, to follow that up India is carrying out some rigorous awareness campaign for the public.

Virus-transfer offences are only dimly known by the general public. They are, however, oblivious to the bigger picture of risks that might jeopardize their online lives. Most internet users are unaware of the dangers of e-commerce and online banking.

b) *Contribute to the worldwide discourse on the emerging jurisprudence of Cyber law* - Nobody knows when, how, or in what way the Internet will be balkanized, if it happens at all. This is a significant issue that demands extensive discussion and debate among all countries. Countries have a special responsibility to ensure that the global Internet is not interrupted in any way.

The International Conference on #Cyberlaw & #Cybercrime will be held in New Delhi on March 13th, 2014, to debate problems relevant to the growing Cyberlaw jurisprudence in a changing world, particularly in the light of the Internet's Balkanization.

The stated Conference is expected to bring up and address various elements and concerns relating to Cyberlaw jurisprudence difficulties. Clearly, the subject of Internet Balkanization and its potential repercussions, both for consumers and for nation governments, are major topics that may be discussed at the International Conference on #Cyberlaw & #Cybercrime.

CRITICAL ANALYSIS

After looking through all of these difficulties, one can only hope that some strict legislation would be enacted in the future to deal with such crimes, as a result of the increased severity of penalty, new legislation for reference, the rate of cybercrime will be lowered, and the period of technical growth and digitalization will be free of evil, thanks to laws that take a specific solution to a specific problem and make the individual majority of punishment non-bailable.

Because cybercrime is easy to commit but extremely difficult to detect, it is critical to have a cyberlaw enforcement movement to combat the increasing trend of cybercrime. Despite India's extensive and well-defined legal system, all current laws were enacted decades ago, taking into consideration the political, social, economic, and cultural conditions of the time. At the time, no one could have imagined the Internet. The needs of cyberspace could never be predicted, no matter how skilled our master draughtsman are. The needs of cyberspace could never be foreseen, no matter how skilled our master draughtsman are. As a result of the growth of various sensitive legal problems and ills, Cyber laws were enacted. Second, even with a liberal

interpretation, the current statute cannot be interpreted in light of emerging internet technologies. The Internet demands a legal framework that is current with the times. Because present laws have failed to create this legal foundation, only appropriate Cyber laws may be enacted. All these circumstances made it necessary for India to pass comprehensive cyber legislation.

CONCLUSION

To deal with the growing problem of cybercrime, the Indian legal system must pick up the pace and make changes to both the legislation and the executionary organizations. Despite India's seemingly well-defined legal structure, this issue warrants additional attention. Even with a broad interpretation, current rules cannot cover all of today's cyber problems. The entire legislative framework must be revised to align laws with today's cyber issues. Finally, failure to deal with this is not an option because it has consequences ranging from daily living to India's national security.