



International Journal of Allied Practice, Research and Review

Website: www.ijaprr.com (ISSN 2350-1294)

An Overview of Cyber law

¹**Naresh Kumar,**

**Lecturer, Government General Zorawar Singh Memorial Degree College Reasi,
Jammu and Kashmir, India**

²**Bindu Jamwal,**

²Teaching Assistant, GDC Plaura, Mishriwala, Jammu and Kashmir, India

³**Jai Kumar,**

Teaching Assistant, GDC Samba, Jammu and Kashmir, India

Abstract - Cyber law's is a term used to cover legal issues related to the use of communication technologies, particularly "cyberspace", i.e. the Internet. It falls under a different legal field in the way property or communications are, as it is at the crossroads of many legal forums, including intellectual property, privacy, freedom of speech, and regulatory authority. In fact, online law is an attempt to integrate the challenges posed by cyberbullying with a legacy system that operates in the physical world. The growth of e-commerce has further enhanced the need for more efficient and effective regulatory systems that can strengthen legitimate infrastructure, which is critical to the success of e-commerce. All of these controls and legal infrastructure fall within the scope of Cyber law. This research paper tends to address the growing and growing problem of cybercrime by taking essentials and qualifications and highlighting their problems.

Keywords:- Cyber law, Cybercrime, Cyberspace, Fakesm

I. Introduction

In today's world of rapid growth Information technology is circulating in all walks of life around the world. These technological advances have made the transition from documentation to paperless communication possible. We are now creating new Tempo Principles, efficiency, and communication accuracy, which have been reflected in the development of design, innovation and product development as a whole. Computers are fully utilized to maintain confidential political, social, economic or sensitive data that brings significant benefits to society. The rapid development of internet technology and computer technology around the world has led to the rise of internet-related. These cases are mainly related to the internet. These cases are virtually unlimited and could affect any country in the world. So there is a need for caution and mandatory law in all States to anticipate cybercrime. Internet and computer-based trade and communications around the world cross-border defenses

thus, creating new governance of human activities, undermining the feasibility and legitimacy of the use of local laws. This novel periphery, made up of screens and passwords, separates the "Cyber World" from the "real world" of atoms. Local-based authorities and law enforcement officials find this new location extremely threatening.

II. Need of Cyber Law

While the internet was being developed, the creators of the internet were not at all inclined to the fact that the internet could transform itself into a ubiquitous revolution that could be misused in criminal activities and required regulation. Today, many disturbing things are happening online. Due to the anonymous nature of the internet, it is possible to engage in various criminal acts with impunity and clever people, who have misused this online feature to promote cybercrime.

III. Importance of Cyber Law

Cyber law is important because it affects almost every aspect of transaction and online and offline activities, the World Wide Web and Cyberspace. At first glance it might seem that Cyber rules are a very technical one and have nothing to do with most jobs on Cyberspace. But the real truth is that nothing can be further from the truth. Whether we realize it or not, every action and every reaction on Cyberspace has certain legal implications with Cyber. It is important to strengthen the negative impacts of the internet and to detect cyber crime.

As the online environment changes and this new approach is seen as the last resort in human history, all your activities at Cyberspace can and will have a cyber legal perspective. From the moment you register your domain, to the time you set up your website, to the time you do electronic transactions in a specified location, at all times, and there are various issues of online law. You may not be concerned about these issues today because you may feel that they have no effect on your Cyber operations. But soon, you will need to tighten your belts and be aware of Cyber law in order to benefit.

IV. Evaluation

Cyber law is constantly changing. As new and new opportunities and challenges arose, Cyber law, which is a ever-changing process, adapts accordingly. As the internet grows, more and more legal issues arise. These issues range from domain names, from intellectual property rights to Electronic Commerce to privacy to Encystations to Electronic contracts to Cyber crime to Online Banking to Spam and soon. The list is too long. Whenever cyber crime changes and the mind of cybercriminals recommends committing cyber-related crimes, Cyber law also seeks to correct crime.

Today, awareness of cyber law is beginning to grow. Many technical experts initially felt that legal regulation was unnecessary. But with the rapid growth of technology and the internet, it is clear that no online activity can remain free from the influence of Cyber law. Publishing a Web page is a great way for any business or company to significantly increase its exposure to millions of people, organizations and governments around the world. It is that aspect of the Internet that has caused much controversy in the legal community.

V. Objectives

As the Internet grows in our country, the need has been raised to establish the appropriate Cyber laws needed to regulate the Internet in India. This need for Cyber rules was driven by a number of factors.

First of all, India has a very detailed and well-defined legal system in place. Many laws were enacted and the most important of which was the Constitution of India. Among other things, among others, the Indian Penal Code, the Indian Evidence Act 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, the Companies Act, and so on. However, the advent of the internet has marked the beginning of new and more complex legal issues. It may be necessary to point out that all existing laws in India were passed back in view of the relevant political, social, economic and cultural situation at the time. No one could really visualize the Internet. Apart from the ingenious ingenuity of our professional designers, the demands of cyberspace were far from anticipated, the advent of the internet has led to the emergence of legal issues and many problems that require the enactment of cyber laws.

Second, existing Indian laws, even the most kind and liberal definition, could not be interpreted in the light of the emerging cyberspace, to cover all aspects of the various functions in the Cyber environment. In fact, practical experience and judicial intelligence found that it would not be without major risks and pitfalls, if existing laws were to be interpreted into the emerging Cyberspace context, without establishing a new Cyber law. Thus, the need for proper cyber law enforcement.

Thirdly, no existing law provides for the legalization or sanction of Cyberspace operations.

Fourth, the Internet needs legitimate and up-to-date legal infrastructure. This legal infrastructure can only be provided with appropriate cyber laws as traditional laws have failed to provide the same. E-commerce, the future of the internet, is only possible if the required legal infrastructure recommends the same to enable its healthy growth.

VI. Cyber Crimes

Common types of Cyber Crimes may be broadly classified in the following groups:-

1) Against Individuals: -

A. Against Person: -

- Harassment through e-mails.
- Cyber-stalking.
- Dissemination of obscene material on the Internet.
- Defamation.
- Hacking/cracking.

- Indecent exposure.

B. Against property of an individual: -

- Computer vandalism.
- Transmitting virus.
- Internet intrusion.
- Unauthorized control over computer system.
- Hacking /cracking.

2) Against Organizations: -

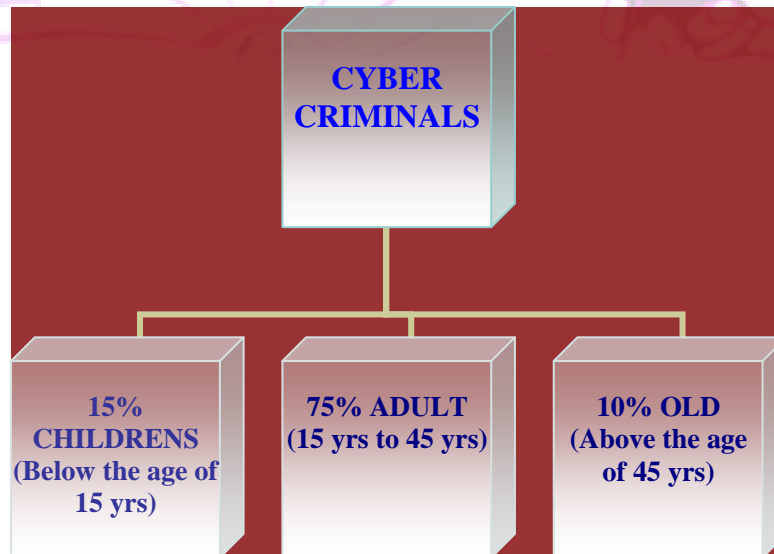
a. Against Government, Private Firm, Company, Group of Individuals: -

- Hacking & Cracking.
- Possession of unauthorized information.
- Cyber terrorism against the government organization.
- Distribution of pirated software etc.

3) Against Society at large: -

- Pornography (especially child pornography).
- Polluting the youth through indecent exposure.
- Trafficking.

Figure 1.1 Cyber crimes on the basis of age group

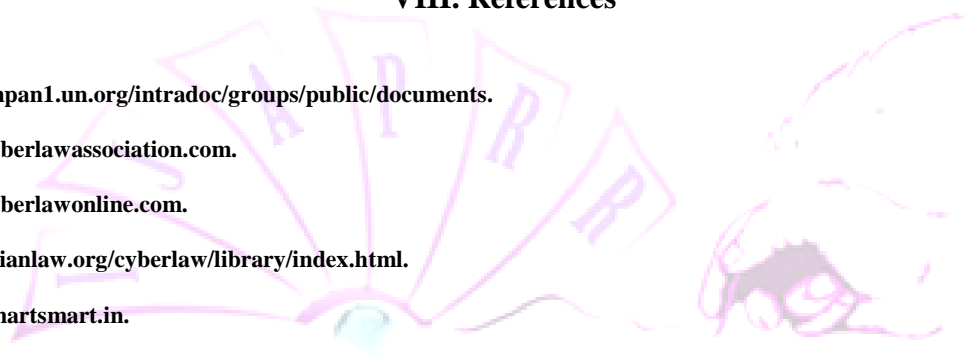


A general comparative analysis of different age groups has been taken (Children, Adult, and Old people)

VII. Conclusions

Therefore, the conclusion may be that a computer-related crime is real, (at least in certain cases) the hardest. In addition, the continued increase in the number of such crimes in the region is predictable which requires better attention from law enforcement officials. Now let us review some of the available ways to establish a comprehensive legal framework. Can we make only local laws that apply to online activities that do not have appropriate or predetermined locations? It seems very difficult. We must also allow responsible online stakeholders to set their own rules and assist all stakeholders (online and offline). Internet law has already emerged, and we believe it can continue to emerge from individual users who vote to join certain systems they find most popular. However, this model also does not solve all the problems, and various management problems cannot be solved in an instant. We will need to redefine Cyber Legal processes in this exciting new context. Finally, the Cyber Law defined as a thought-provoking group discussion about core values and the unique benefits of the Organization will continue. But it will not, will not, and should not be the same law that applies to real, geographically defined areas.

VIII. References

- 
- [1] www.unpan1.un.org/intradoc/groups/public/documents.
 - [2] www.cyberlawassociation.com.
 - [3] www.cyberlawonline.com.
 - [4] www.asianlaw.org/cyberlaw/library/index.html.
 - [5] www.smartsmart.in.
 - [6] www.indii.org/cyberlaw.aspx.
 - [7] Cyber Laws: provisions and preventions by Tariq Hussain.
 - [8] www.free-articals-searc.com.
 - [9] www.cyberlawcentral.com.
 - [10] www.thisbooksshop.com
 - [11] www.csdms.in.
 - [12] www.cyberlawenforcement.org.
 - [13] www.cyber.law.harvard.edu.