International Journal of Advance and Applied Research (IJAAR)
Peer Reviewed Bi-Monthly

ISSN – 2347-7075
Impact Factor – 7.328
Vol.9 No.4 Mar – Apr 2022

A STUDY ON AN EMERGING CYBER LAW ISSUE

Mrs. Sheetal Khetiya

Ph.D. Research Scholar,
Department of Law,
Shri. J.J.T. University, Rajasthan, India

ABSTRACT:

Today, everyone is moving towards the era of digitization and networking, which has various benefits in a variety of sectors like e-commerce, communication, and so on and so forth. In an instant, it also gives rise to a whole new criminal strategy that has come to be known as cybercrime. A concentration on the accompanying norms and orders is required if crimes are to be avoided in an environment as virtual as this one. The Information Technology Act of 2000 and the National Cyber Security Policy are just two examples of the many laws and measures that have been established and put into place to fight these issues. Acts such as "cyber vandalism," "cyber violence," and "cyber rape" are not considered to be "cybercrime" and have no legal importance, despite the fact that the term "cybercrime" does not have a meaning in legal parlance. The issues that exist in cyberspace are the primary subject of this research. Particular attention is paid to the pressing need for modifications to India's existing cyber legal system, as well as several circumstances in which cyber law enforcement falls short.

Keywords: *Cyber law, Cybercrime.*

INTRODUCTION:

In terms of the scenario of technological growth, it is happening all over the globe, and it is doing so in a very swiftly expanding and very positively manner. However, with this, a few of negative things come to the forefront as well. One of the features is the rapidly accelerating rise of digital and network technologies, which contributed to the development of a cyberspace equivalent of a virtual world. The expansion of cyberspace brings about a boom in every aspect of lifestyle and the business, but at the same time, there is a rise in a new kind of crime that is known as cybercrime. The Internet was first designed as a tool

for study and the dissemination of information; nevertheless, it is now either the tool of the target or both when it comes to committing cyber crime. As more time passed, it grew more transactional with communication, online shopping, electronic government, and other such things. Cyber laws address every single legal problem that arises out of criminal activity on the internet. As the number of cybercrimes such as unauthorised access and hacking, Trojan attack, virus and worm assault, denial of service attacks, and so on continues to rise, the need for relevant legislation and the execution of such laws has also amassed a significant amount of momentum. The genesis of cybercrime is unknown, and there is no precedent for it in legal precedent. During the tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, there was a session that was dedicated to the concerns of crimes connected to cyber space. During this workshop, cybercrime was classified into two categories and characterised as follows:

a. A restricted definition of cybercrime refers to any criminal activity that is carried out via the use of electronic operations with the intention of undermining the safety of computer systems and the data that is being processed. This kind of computer crime is known as cybercrime.
b. In a broader sense, the term "cybercrime" refers to any illegal behaviour that is committed by means of an operating system or network. This can include illegal possession of information or the distribution of information by means of a computer system or network. Cybercrime falls under the category of computer-related crime.

Attacks against digital networks with the objective of capturing control of or even destroying infrastructures that are critical to governments and sectors are of the utmost significance, according to the tactical perspective. According to the Norton analysis, the frequency of cyber assaults on Indian assets is overstated, with both the private and public infrastructure being targeted. After the publication of the government's national cyber security strategy in July 2013, it was immediately revealed that government officials' emails had been hacked shortly afterwards. The NCSP does not even come close to addressing all of the complexities of the cyber threat. It only gives general guidance for how the

standard operating procedure should be carried out; it does not make the most of its potential for the greatest possible advantage. The most important security problem relating to the telecommunications business, which is now completely interwoven into the online world, is absent.

It is anticipated that the number of crimes of this kind committed in this region will continue to rise, which calls for more attention from the legislative body.

LITERATURE SURVEY:

The proliferation of illegal behaviour coincides with the development of new technologies; the Information Technology Act of 2000 outlines strategies for combating cybercrime. Although there are certain advantages to be gained by using this paradigm from an e-commerce point of view, it is not a panacea that will immediately address all of the challenges and concerns. [1] The IT Act is regarded to be a vague piece of legislation due to the fact that the area of authority in relation to the internet is uncertain. It is difficult to erase information from a computer system in the virtual world of cyberspace, which is why computer forensics is becoming increasingly important in the field of investigating evidence of cybercrime. In order to properly handle computer forensics, one needs to be an experienced and knowledgeable computer expert because the slightest mistake can result in the destruction of evidence. [2] Despite the fact that the Information Technology (Amendment) Act of 2008 addresses further issues, the Indian Penal Code does not utilise the word "cybercrime" at any time. After the year 2008, it is clear that there has been a rise in the amount of cybercrime that has been committed as a result of criminals finding loopholes within the law and then engaging in illicit activities. The victim of a cyberattack might be an individual, their property, or the government. [3] There are not many judicial precedents to look to for direction, and the existing rules did not sufficiently address the nature of the crime that was being committed. There is a pressing need to advance cyber legislation. Our legal system should provide for severe punishments to ensure that criminals serve as effective deterrents for other potential offenders. [4] The Information

Technology Act (amendment) of 2008 expanded the jurisdiction of cyber law. An amendment was made to the defining portion of the evidence legislation. [5] The territorial jurisdiction problem is a key one that the Information Technology Act of 2000 does not solve adequately. It is common knowledge that investigators often avoid taking complaints on the grounds that they fall within the jurisdiction of another agency. [6] The development of India has not been accomplished in every facet, including e-courts, online dispute resolution functions, effective cyber legislation, cyber forensics, and other areas. Revision of the IT Act is required. In addition, there should be greater emphasis in India placed on the provision of scientific and technical professional training for lawyers. [7]

Due to the geographically indeterminate nature of the internet, cybercrime is one of the emerging trends in criminal activity that has the potential to affect every facet of human life. Although it is simple to commit, cybercrime is notoriously difficult to uncover, and authorities frequently struggle to pinpoint its origins in terms of legal jurisdiction. [8] There is a need for cyber security in order to safeguard the developing ICT. The knowledgeable group needs to investigate the essential information and communications technology (ICT) systems that are supporting the nation's governance structure and provide recommendations on an appropriate mix of solutions. [9] Acquiring a knowledge of the danger posed by cyberspace and acquiring the capability to take offensive operations inside this cyberspace is an absolute need. As a result of the fact that nations, non-state actors, terrorist organisations, groups and people pose a threat to development, which is increasingly going to be reliant on the cyber domain, it is necessary to identify technologies in this respect. [10]

The term "adversary" refers to any individual who engages in harmful behaviour. Both insiders and outsiders may play the role of adversary. The opposite of an insider is an outsider. One who has authorization to enter a nuclear plant or sensitive activities is considered an insider. They complemented one another using their authority, such as the power to obtain entrance. Cybercrime is a multi-billion dollar issue, and if we want the benefits of the computer era without the downsides, we need to implement strong laws to

prevent the benefits from being overshadowed by the negatives. [11] Governments and commercial companies all across the globe are very concerned about their level of cyber security. The term "cyber threat" may refer to an actual cyber assault, but it can also refer to the potential consequences of "mistakes" or even natural catastrophes. Therefore, within the scope of cyber security, there must to be a specialised response to the particular situation. [12] There are several problems that need to be solved in cyberspace, including as the legal issues with cyber security, the span gap, the legal issues surrounding cloud computing, the obstacles that mobile law presents, and the legal issues surrounding social media.

In order to keep the con artists at bay, the producers will need to go the additional mile, and it should be the responsibility of three stakeholders:

- the user, the ruler, the regulators, and the law makers all have a responsibility to play in ensuring information security in their various capacities, whether they be the internet service provider, the network service provider, or the bank.

CYBER LAWS:

In the 20th century, a number of new preconditions and infractions were added to the legal lexicon. Because it is vitally essential to realise that a computer cannot commit a crime but that humans may, legal measures should give assurance to users, deterrent to criminals, and deterrence to enforcement authorities. People, not robots, are the ones that misuse, destroy, and skew the information that they have access to. The United Nations Commission on International Trade Law (UNCITRAL), after understanding the need to battle with the cyber violations, developed the Model Law of Electronic Commerce in 1996. This was done in recognition of the need to combat with the cyber violations. After that, the General Assembly of the United Nations issued a recommendation suggesting that all governments should look favourably on the State Model legislation and give it favourable attention. In the course of carrying out its responsibilities, the Government of India acknowledged the need of passing law and moved on with the introduction of a brand new piece of

legislation in the shape of the Information Technology Act, 2000. It was strengthened by the revisions that were made to it. Following the passage of the Information Technology Act, the principal legislation that were subject to revision are the Indian Penal Code (e.g. 192, 204 ,463, 464 , 468 to 470 , 471 , 474 , 476 etc) Before the passage of the Information Technology Act (IT Act), all of the evidences that were presented in a court were in physical form. Only after the passage of this law were electronic records and documents acknowledged. The following topics are covered in significant detail by the Act:

- Legal identification of Electronic document.
- Legal identification of Digital Signatures
- Offenses and Contraventions Justice
- Dispensation Systems for cyber crimes

From the point of view of electronic commerce in India, the Information Technology Act of 2000 contains many positive aspects. For example, companies shall now be able to carry out electronic commerce using legal infrastructure for the authentication and origin of electronic communication through digital signatures. Additionally, the act makes an effort to change outmoded laws and provides ways to deal with cybercrime. However, it is regarded to be the legislation with the most grey areas in the field of authority when it comes to the Internet. Because subsection (2) of section 1 specifies that the act is to be extended to the whole country of India, and unless otherwise specified in this Act, it applies to any offence or violation of the terms of the act that is committed outside of India by any individual. This act shall apply to an offence or contravention committed outside of India by any person if the act or behaviour constituting the offence or contravention includes a computer, computer system, or computer network that is situated in India, as stated in section 75 (2). It would seem that this kind of provision is in conflict with the notion of fairness. In point of fact, the phrase "cybercrime" may be used at any time, even after it was modified by the IT Act Amendment in 2008. There is a pressing need to move cyber legislation forward.

VARIOUS ISSUES UNDER CYBER LAW ENFORCEMENT:

Issues related with law:

- In the Information Technology Act, territorial jurisdiction is not adequately addressed because it is mentioned in sections 46, 48, 57, and 61 in the context of the adjudication process and the appellate procedure connected with, and it is mentioned once more in section 80 as a component of the police officer's authority to enter and search a public place for evidence of cybercrime, among other places. It is difficult to determine which police station will have jurisdiction over a cyber crime given that these offences are fundamentally computer-based. This makes it difficult to know which police station will be responsible for the investigation because, in general, investigators try to avoid accepting complaints based on grounds of jurisdiction.
- In contrast to crimes that take place in the real world, where tangible evidence such as the weapon used in the crime, finger prints, and other such things are simple to find and present in court, it is challenging to remove information from a computer system in the virtual world, contrary to what is generally thought to be the case. The field of computer forensics is used to accomplish this task. And the process of preserving evidence related to cybercrime belongs with the competent computer forensic expert since any negligence in the process may lead to a diminution in the value of the evidence. This is why the procedure lies with the expert. However, it is very important for the victim to notify the appropriate law enforcement agency as soon as possible.
- In order for specialists to effectively combat cybercrime, they need not only to have extensive knowledge but also to have access to the appropriate technological devices and software.
- The old laws are not competent for the crime that is being perpetrated in the present environment, and the new laws hadn't fully caught up to what was occurring. This leaves law enforcement personnel without the tools they need to do their jobs.

- There is a lack of collaboration between the authorities that police the law and those who work in the computer industry.
- Even with the IT (amendment) legislation of 2008, the International Criminal Code does not include the word "cyber crime" anywhere in its text.
- The lack of care for security in the telecommunications business, which is integrated into cyberspace and has an additive impact of Internet protocol on mobile devices, is often regarded as the key cause contributing to an increase in the number of assaults.

Issues related with the technology:

The adoption of new technologies like cloud computing for e-governance and data storage raises serious concerns about the potential for cyberattacks. The efforts that have been made to meet the problems and risks of cloud computing, such as, have not been effective.

- The possibility that private and sensitive information might be accessed inappropriately. There is a possibility that sensitive information and intellectual property may be revealed. It is necessary to put in place the appropriate privacy and safety precautions.

Big data, another kind of developing technology that is now seeing a lot of application, poses significant threats to users' personal information and privacy. From the perspective of business, a great number of works have been produced that centre on the processing of information derived from business applications and big data. It is up against a number of obstacles, including techniques for efficient encryption and decryption, retrieval of encrypted information, and maintaining the dependability and integrity of Big Data.

According to the record of the 52nd report of the standing committee on information technology (2013-14), the following is the total number of offences that were documented under the IPC and the IT Act of 2000:

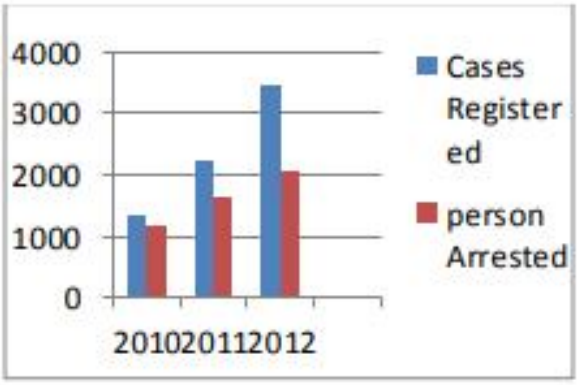

Figure 1: Shows offences registered and the person arrested

The graph that appears above displays a comparison between the number of offenders arrested under the IT Act 2000 and the number of offences recorded under the IPC. The results of a cursory investigation reveal the truth behind the scenes, namely that the number of offences reported increased from 1322 in 2010 to 2213 in 2011 to 3477 in 2012. However, the number of people arrested increased to 1630 in 2011 and 2071 in 2012 from 1191 in 2010. This paints a very obvious image that there are a variety of problems in law enforcement that need to be resolved in order to put an end to crimes of this kind.

PROPOSED IDEOLOGY:

IT Act is considered to be the toothless so there is need to strengthen it as:-

- IT Act (amendment) Act 2008 reduced thequantum of punishment for majority of cybercrime. Need to be rectified. Majority of cyber crimes need to be made
- non-bail able offence. There is need to cover cyber war under IT
- Act as an offence.

In order for the legislation to have the desired impact, a data protection regime has to be implemented into it. The record of the 52nd report of the standing committee on information technology (2013-14) indicates that the rate of hacked websites, among which there were also government websites, was as follows:

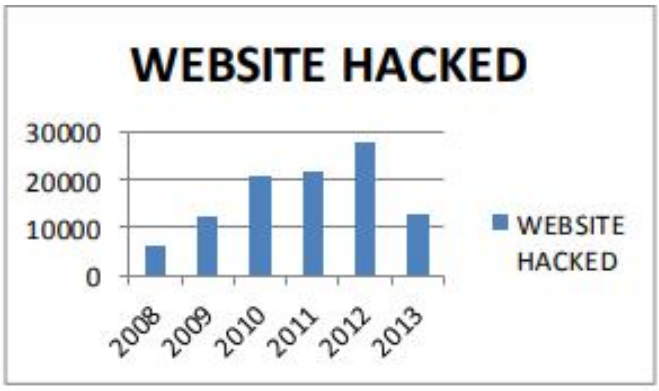

Figure 2: Shows websites hacked during the year 2008-13

According to the figure that was presented earlier, the following is a scenario that states the number of websites that were hacked in 2008 was 6310, in 2009 it was 12161, in 2010 it was 20701, in 2011 it was 21699, in 2012 it was 27605, and in the year 2013 up to June, its number is 12693. This is a scenario that was presented earlier. The figures presented here make it very evident that criminal activity committed online is on the rise. Not only is this an issue with regular websites, but the same danger is also growing for official government websites. The following figure will provide a more robust understanding of the same.

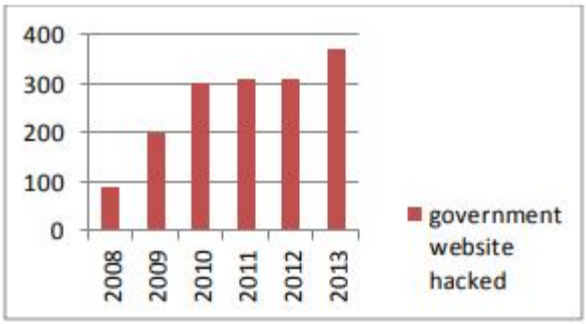

Figure 3: Shows number of government websites hacked during years 2008-13

According to the previous statistic, the following is a scenario that states the number of websites that were hacked in 2008 was 90, in 2009 it was 201, in 2010 it was 303, in 2011 it was 308, in 2012 it was 308, and in the year 2013 up to June, its number is 371. In other words, the number of websites that were hacked increased by 91 percent from 2008 to 2009. According to these findings, it is abundantly obvious that the rate of cybercrime is rapidly increasing, and this

is true for both the regular world and the government's virtual world. People who commit crimes pose a threat to the nation's security in a roundabout way. As a result, it is necessary to take some severe actions in order to put a stop to such a heinous sickness.

One has a responsibility to make sure that the system provides severe punishments for those who commit cybercrimes and for those who commit cybercrimes, so that others are discouraged from doing the same. In order to achieve the desired outcomes, the NCSP's adopted policies had to be made legally enforceable.

New cyber law jurisprudence should be set up. Also, International court for cyber security should be set up.

CONCLUSION:

It is essential to have a momentum for enforcing cyberlaws in light of the rising trend of cybercrimes. This is due to the fact that cybercrime has the potential to harm every facet of life, despite the fact that it is simple to do but very difficult to detect. Although India has a legal system that is extremely detailed and well-defined, all of the laws that are currently in effect in India were enacted in the past with the political, social, economic, and cultural climate of the time in mind. This is despite the fact that India has an extremely detailed and well-defined legal system. Back then, nobody could fully fathom what the Internet would be like. In spite of the extraordinary competence of our master draughtsmen, it seemed quite unlikely that the requirements of cyberspace would ever be anticipated. As a consequence of this, the introduction of the Internet resulted in the formation of a great number of contentious legal problems and ills that called for the establishment of cyber laws. Second, even with a liberal interpretation, the legislation that is now in place is unable to be understood within the context of the developing internet. The Internet calls for a tenacious and accommodating legal architecture that is in tune with the times. As a result of the failure of the current laws to contribute in the same way, the only way to provide this legal framework is via the introduction of the relevant Cyber laws. The cumulative effect of these several factors produced an

environment that was favourable to the proposition that India need to pass pertinent cyber legislation.

REFERENCES:

1) Maneesh Taneja and Dr. D.B Tiwari,"Cyber Law", International Referred Research Journal, vol.11 (21) October, 2010, pp. 63-65.
2) 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.
3) 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.
4) Talwant Singh, "Cyber Law and IT" pp. 1-4
5) Rohitk.Gupta, "An Overview of Cyber laws vs. Cybercrimes: In Indian Perspective", 2013.
6) Rohit k Gupta, "An Overview of Cyber law vs. Cybercrimes", 2013.
7) 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.
8) 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.
9) M.M.Chaturvedi, M.P.Gupta and Jaijit Bhattacharya "Cyber Security Infrastructure in India : A Study"pp.1-15
10) IDSA Task Report, "India's cyber security challenged" March, 2012
11) Angshuman Jana and Kunal Kumar Mondal, "A survey of India Cyber Crime and Law and its prevention approach" 'International journal of Advance Computer Technology'.
12) David Satola and Henry L.July , "Towards a Dynamic Approach to Enhancing International cooperation and collaboration in Cyber Security Framework", 'The MW. Mitchell law journal'