VOLUME 29 | MAY, 2022 ISSN 2456-9704

PREVAILING CYBER SECURITY LAW

By Shruti
From Netaji Subhas University, Jamshedpur, Jharkhand

By Ashutosh Kumar
From Netaji Subhas University, Jamshedpur, Jharkhand

By Adv. Priya Ranjan
Advocate, Jharkhand High Court

ABSTRACT

The term cyber-security has emanated from a research project on ARPANET (The Advance Research Projects Agency Network), predecessor of the internet that exists today. The roots can be traced back to 1970's when the first ever antivirus came to existence. Computer security or Cyber security basically implies defense from breaching of data, its thievery or mutilation, whether in regards of software or hardware. In a world that is heading towards the age of digitalization, a risk of being caught off-guard on the cyber space always lurks in the digital space. With advancing virtual exploit the modern laws need to catch up with the ever-increasing cybercrime rate. The punishments regarding cybercrime are available in the IT Act of 2000.The law covers every aspect of technology viz. computer networks, processing devices, software and storage. Safeguarding the information technology can be deemed as the core purpose of cyber security. The benefits can be rated as per the services being provided such as the anti-virus software, encryption, fire walls, and login passwords. Regardless of the former data protection systems there have been cases of information theft and mutilation. That's where the cyber law comes in for the defense of an individual. The cybercrime law has a history of its own and has been through a process of evolution to meet the demands of modern era, changing the already existing traditional laws in the due course. There is no statuary definition for cybercrime under Indian laws.

Keywords: Cyber, Security, IT Act, cybercrime, technology, digitalization.

INTRODUCTION

Information Technology refers to computer system their hardware, software including networks, internet together with various applications running on the internet. Primarily consisting of devices used for storing, retrieving and transmitting information.[1]

Another concept that concurrently occurs with the former is "Cyber space". It is an assembly of intangible objects, like websites, social networks, and blogs etc. It can be presumed as a virtual space without any geographical barrier where all of the IT associated communication and actions are taking place. Marshall McLuhan in his book 'Understanding Media' (1964) coined the term "global electronic village" for cyber space.

The augmentation of 'IT' has been followed by proliferating cybercrime rate. It can refer to as an unauthorized access to computer

[1] www.techtarget.com (Dec. 8, 2021, 8:01 PM), https://www.techtarget.com/searchdatacenter/defination/IT.

system and personal data, breaching of data, its manipulation or misuse. The Protection of probity of all lawfully created computer, its system and data are crucial as far as the wellbeing of all the entities who are utilizing the cyber space is concerned. The laws governing the physical world are not apt for the cyber world where the objects are impalpable therefore the ordinance of the cyber space should be specialized. [2]

IT has alleviated our lives. It has also made crime easier. There are no physical barriers fending off criminals from committing virtual offenses, it can be perpetrated from anywhere and anonymity can be maintained during the process. Its accessibility is also a cinch because of low cost of IT. It has also brought forth a divergence by escalating the traditional crimes (cheating, theft) along with new age crimes viz. Computer hacking , Phishing, Malicious software, Disturbed denial of service(DDOS) and Data stealing. These crimes can range from basic computer crimes to organized crimes like drug trafficking, extortion, software piracy *etc.* The 'IT' exploit has spread the risk to Computer/computer system/Information, financial risk, Individual and risk so on. [3]

There are several points worth mentioning which gave rise to this stream of laws or Cyber laws.

- Cyber-crimes being immune to geographical barriers creates ambiguity when a crime is committed from a different territory or country to another, for example a crime committed in US and its impact is felt in India.
- Creation of new crimes that are not recognized by conventional laws, for instance overloading of a website with requests hindering or blocking it from functioning.
- Intangible nature of the cyberspace makes traditional methods of gathering evidence abortive.
- Netizens can use fake identity or a replica of someone's identity making evidence collection challenging.
- The immense volume of data is hard to keep track of.[4]

The former reasons led to enforcement of specialized laws to provide fair and effective criminal justice procedures by establishing limpid standards of behavior for the use of computer devices, safeguarding individual's identity while investigating, dissuading the malefactor and allowing cooperation between countries in criminal proceeding involving cybercrime and electronic device. The IT Act (2000) in India lay out the legal framework required for e-governance through providing identity to electronic records and digital signatures. It elucidates the cybercrime and specify the penalties. Currently the IT Act consists of 13chapters and 90 Sections.[5]

[2] www.techopedia.com (Dec. 8, 2021, 8:20 PM), https://www.techopedia.com/definition/2493/cyberspace.

[3] www.nationalcrimeagency.gov.uk (Dec. 8, 2021, 8:35 PM), https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime.

[4] ANIRUDH RASTOGI, CYBER LAW: LAW OF INFORMATION TECHNOLOGY AND INTERNET (1st ed. 2014).

[5] www.cyberlawsindia.net (Dec. 9, 2021, 7:22 PM), https://www.cyberlawsindia.net/cyber-india.html.

(A) Literature Review

While researching any topic it is necessary to find out the research problems on which a researcher wants to work. After analyzing the research problem, a researcher needs to find out the solution of these problems for which he needs to do the research and he has to go through different books, reports, journals, magazines, articles and research papers. Now after going through all these a researcher gets clarity on the concerned topic. There are several pieces of literature available on the concerned topic i.e., cyber-crime, which shows that a lot of work has already done on the topic and several books were also published. Here, In this paper, the researcher tried to attempt to review the literature of some authors.

1) **Justice Yatindra Singh** in his book **"Cyber Laws"**[6] talks about the cybercrime-related to Intellectual Property right i.e., Trademark, Copyright, and Patents etc. According to Justice Yatindra Singh, Intellectual property rights refers to all the property which is a creation of the mind. It means that all those things are created by way of invention, literary, and artistic works. For example, design of a symbol, cinematography, sound recording, photography, writing books, making songs and films, and making designs which are used for different purposes such as commercial like the logo of Amazon etc.[7] Justice Singh in his book explaining the science behind the new emerging technology. While discussing the Information and Technology Act, 2000 and its amendments in 2008, he explains the meaning and concept of digital signature, electronic signature and all the relevant provisions relating to it including with procedure of authentication and recognition of it. He, in his book, talked about cyberspace and its intermediaries and also analysed the crimes given under the Amendment Act of 2008.

2) **Vakul Sharma** in his book **"Information Technology**: **Law and Practice"**[8] explain the role of Information and Technology in practice and its laws related to it. In his book, he has given many examples which makes his book easier to understand for a reader. The issues related to the jurisdiction in cyberspace and its laws have been discussed in his book very precisely. To understand the concept of jurisdiction, he discusses different principles such as territorial principle, protective principle, passive personality principle nationality and universality principle. He, in his book, quoted several Supreme Court judgements to justify the legislation behind the cyber laws and its true intention of the legislation. Also, discussing the different case laws related to cyber-crime referred by him helps to under the concept and the provision and interpretation of cyber-crime and its laws. In his book, he critically analysed the police, the tribunal and the adjudicating authorities related to cyber-crime. He criticises by relying upon the technology and technical training given to these authorities.

3) **Dr Jyoti Rattan** in her **book "Cyber Laws & Information Technology"**[9] , She, in her book explained the very concept starting

[6] Justice Yatindra Singh, Cyber Laws, (Universal Law Publishing Co. Pvt. Ltd., 2010).
[7] Ibid, p. 45.
[8] Vakul Sharma, Information Technology: Law and Practice, (Universal Law Publication, Co., Delhi, 2010).
[9] Dr. Jyoti Rattan, Cyber Laws & Information Technology (Bharat Law House Pvt. Ltd., New Delhi, 2014).

from the evolution of computers and everything about computer and their components, their advantages and disadvantages. She very well explains the emergence of IT, network and cyberspace with different examples, which help us to understand everything very well and in an explained manner which makes it more interesting and comprehensible. As in the book of **Vakul Sharma**, the jurisdictional aspect has been dealt with. She also explained it in a very comprehensive manner both at the national and international levels. She, in his book, explains the civil liabilities as well as criminal liabilities. According to her, the use of a computer to carry out any conventional criminal act is called Cyber Crimes. Cybercrimes are aimed at stealing the computer, damaging information or stealing information.

She has classified cybercrime basically into six categories based on:

1) Old and new Crimes Committed on computer.
2) Victim of cybercrime.
3) Nature of Cyber Crime
4) Role of Computers.
5) Source and Motive
6) Criminal activities.

She mentioned the offences which are given under the Information Technology Act, 2000 and also critically analyse them.

4) **Dr. Krishan Pal Malik** in his book **"Computer Information Technology Law"[10],** he, in his book, basically given the statistics on cyber crimes and their reports, and the person arrested for the violation of it. He also explains the definition of computer and information technology in his book. He also explains cyberspace, the fundamentals of the internet and the historical background of such crimes. He explains the ideology and good thought behind implementing the Information Technology Act, 2000 and its amendments. Basically, in his book, he explains the computer as a prime element of such crime and also classified the crimes into different crimes and at last but not least he explains the investigation procedure and legal provision related to cyber-crime and its laws.

5) **S.K. Verma** and **Raman Mittal** in their book **"Legal Dimensions of Cyber Space"[11]**, has explained the meaning and the concept of the computer and internet and its development starting from history to the present. They made a detailed and comprehensive study on cyberspace. They have well explained the terms related to cyberspace. While emphasizing the importance of the computers and internet in day-to-day life they have mentioned that "today it touches and influence almost every aspect of our lives. We are in the information age and computers are the driving force.

(B) Hypothesis

Hypothesis means an idea, supposition or proposed explanation which is made as a starting point of further investigation without any assumption of its truth based on limited evidence or reasoning power. In simple words, it is a tentative statement the validity of which is yet to be tested. It may be proven correct or wrong because it is based on a supposition which is provisionally accepted

[10] Dr. Krishan Pal Malik, Computer Information Technology Law (Allahabad Law Agency, Faridabad, 2010).

[11] S.K. Verma and Raman Mittal, Legal Dimensions of Cyber Space (Indian Law Institute Publication, 2004).

to interpret certain events or phenomenon and to provide guidance for further investigation. The hypothesis formed for the present study is mentioned as under:

a) The ***Lack of comprehensive cyber legislation and lack of proper implementation of the existing Cyber Laws*** in India.
b) Indian Cyber Laws is much weaker than the US cyber laws.
c) The ***lack of cyber courts and proper technical training*** to the concerned department or authority is also not sufficient.

(C) Research Question

a) What is Cyber Crime and how it is discussed in different countries.
b) What is the position of India related to Cyber Crime.
c) How are the regulations are different in different countries.

(D) Research Methodology

The research methodology which is used to write this paper is doctrinal or non-empirical. This paper will analyse the existing statutory provisions and case laws by applying reasoning and analysis. It has been attempted in this paper to verify all the hypotheses through reasoning and analysis with the help of primary and secondary sources, such as legislation, case laws, textbooks on law, commentaries and official websites etc.

CHAPTER 1: The Evolution of Cyber Law

The Computer Fraud and Abuse Act (CFAA) of 1986 was enacted in US as an amendment to prevailing computer fraud law and got incorporated with Comprehensive Crime Control Act of 1984.The law was basic refraining from accessing a computer system without proper authorization. The proportions that the law covered wasn't sufficient to encompass the growing cybercrime activities.[12]

In the case *Rv. Gold & Schifreen (1988)* [13] the defendants had attained unauthorized access to a computer network. The language of the Forgery and Counterfeiting Act (1981) was not intended to apply in the existing case, this resulted into a serious difficulty for both judge and jury. In order to avoid such scenarios from emanating again in the future and hazards of cybercrime with inadequate existing laws, the legislature of Great Britain enacted Computer Misuse Act (1990) .It was able to recognize offences like unauthorized access to computer material, illicit access to commit further offences and unlawful acts with an intention of impairment of operations of a computer.

With Globalization advancement in business, the international community embarked upon the idea for creation of a set of uniform standards for the electronic commerce. This led to sanctioning of the UNCITRAL Model Law on E-Commerce by the U.N. General Assembly. This laid down the following principles

- Non-Discrimination: Excluding any form of discrimination between electronic and physical document. The electronic

[12]https://searchcompliance.techtarget.com (Dec. 9, 2021, 7:35 PM), https://searchcompliance.techtarget.com/definition/The-Computer-Fraud-and-Abuse-Act-CFAA#:~:text=The%20Computer%20Fraud%20and%20Abuse,protected%20computer%20without%20proper%20authorization.

[13] Regina v. Gold and Schifreen,2 WLR 984 (1988)

documents validity can't be denied just because it's in non-physical form.

- Technological neutrality: The provisions adopted in a law are ought to be neutral when technological involvement is there. This ensures swift advancements in technology doesn't make the law invalid after a period of time.
- Functional equivalence: There are certain terminologies via. 'Writing', 'signed', 'original', etc. which are particular to physical document and hence these principles are corresponding criteria for electronic communication. For instance, the original document in physical form would refer to the one originally issued not the copy or Xerox of it, likewise original electronic document implies the one which was first generated in its final form.[14]

First Cyber law of India: The Information Technology Act, 2000

The information technology act is presumed to be an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the model law on electronic commerce on International Trade Law. With international recognition of electronic transactions, the Indian legislature acknowledged the need for a legal framework for e-commerce and digital signature leading to enactment of India's first cyber legislation: the Information Technology Act, 2000 (IT Act).[15]

The purview of the 'IT Act' is to permit the authentication of electronic record by digital signatures, recognition of filing of forms, receipt of payment. It defines the rules associated with electronic records, it defines offences and specify penalties, it establish a Cyber Appellate Tribunal, prescribe extra territorial jurisdiction for cyber felony.

The provisions of the IT Act are not applicable to instruments like a power of attorney, a trust, a negotiable instrument, any testamentary disposition, any contract for the sale or conveyance of immovable property.

In the course of achieving the objectives under the IT Act there were certain amendments required to be made corresponding to the other laws. To imbed the concept of non-discrimination between regular document and electronic documents validity following amendments took place.[16]

Indian Penal Code 1860: References to the term 'document' was amended to incorporate 'electronic records' in it. Extra territorial jurisdiction of IPC was stretched to include all offences keeping on target all the computer resources of India. Finally, sections in relation to a false document were amended to include references to a faulty electronic record.

Indian Evidence Act, 1872: The very definition of 'evidence' was amended to add electronic records. Including some major sections being inserted on admissibility of electronics records, proof and verification of digital signatures.

Banker's Book Evidence Act, 1891: Amendment was made in in the definitions of 'bankers book' and 'certified copies' to

[14] ANIRUDH RASTOGI, CYBER LAW: LAW OF INFORMATION TECHNOLOGY AND INTERNET (1st ed. 2014).

[15] www.cyberlawsindia.net (Dec. 9, 2021, 9:08 PM), https://www.cyberlawsindia.net/Information-technology-act-of-india.html.

[16] ANIRUDH RASTOGI, CYBER LAW: LAW OF INFORMATION TECHNOLOGY AND INTERNET (1st ed. 2014).

include the data stored in electronic devices and printouts of such data. Insertion of a section of certification to follow such printouts was also introduced.
Reserve Bank of India Act, 1934: The powers to make regulations were amended to insert regulations on financial transactions via electronic means.[17]

CHAPTER 2: CYBER CRIME

A cybercrime comprise of any crime which involves a computer system or network, where such system or network is vulnerable to a crime (e.g. Hacking), a tool of crime (e.g. Credit card fraud) or as a repository of evidence related to the crime(e.g. information saved in a computer that aids the investigation). As cybercrime may include conventional crimes such as theft, fraud and extortion this may lead to application of cybercrime specific legislation which is the IT Act along with the application of general criminal legislation i.e., Indian Penal Code,1860 and other laws.

IT Act contains prescription for both offences and contraventions. A contravention implies a violation of a provision of law resulting in a suit in a civil court, offence on the other hand is more consequential violation of law resulting in prosecution in a criminal court. Section 43-45 of IT Act deal with cyber contraventions and section 65-67 deals with Cyber offences.[18]

(2.1) Cyber Contraventions

Section 43: The section defines penalty and compensation for damage done to a computer, computer system, etc. If a person destroys, conceals, alters or steals or causes any other person to cause such damage, that person will be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.[19]

Section 43A: This section of the act deals with punishment to a body corporate that is negligent in implementing/maintain reasonable security practices while possessing, dealing or handling of sensitive information related to a computer resource which it owns, controls or operates and that negligence results into wrongful loss or wrongful gain to other entity.[20]

Section 44: This section penalizes a person in case of failure to furnish any document, return or report to the controller or the certifying authority, failure to file a return or provide any information within the time period specified, failure to maintain books of account or records.[21]

Section 45: This section covers the violations or contravention not applicable under Sections 43,43A and 44. The maximum penalty or compensation of Rupees 25,000 can be charged under this.[22]

[17] www.meity.gov.inU (Dec. 11, 2021, 6:20 PM), https://www.meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf.
[18] www.bbau.ac.in (Dec. 11, 2021, 6:20 PM), https://www.bbau.ac.in/dept/LAW/TM/1.pdf.
[19] IT Act 2000, No. 21, Acts of Parliament, 2000(India).
[20] Ibid.
[21] Ibid.
[22] IT Act 2000, No. 21, Acts of Parliament, 2000(India).

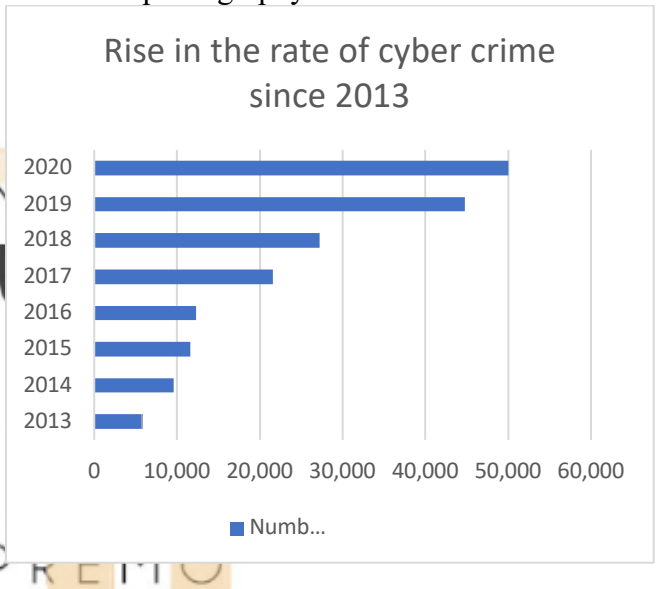
(2.2) Cyber Offences

Section 65: This section deals with alteration of computer source code i.e. it criminalizes direct or indirect concealment, destruction of the source code that is required to be kept/maintained by law in force. The offender must have an intent or knowledge of the crime. This act is punishable with imprisonment of up to 3 years, a fine of Rupees2,00,000 is chargeable ,or both.[23]

Section 66: This criminalize the cyber contraventions under section 43of the Act, in case they are committed with a criminal intent, i.e., dishonestly or fraudulently. In case of Section 43 the act was committed without the requisite authorization and without specifying the *Mens Rea (Guilty mind)*. The penalty involves imprisonment up to 3 years or a fine of Rupees 5, 00,000 or both. The terms 'dishonestly' and 'fraudulently' have been explained in such a way to have the same meaning as that under IPC.[24]

Section 67: This deals with punishment for publishing or transmitting obscene material in electronic form. It was its sole purpose prior amendment, it included all forms of obscene publications, encompassing those related with pornography and child pornography. The punishment prescribed was up to 5 years and Rupees 1 lakh for the first conviction and on subsequent conviction it will get raised to 10 years imprisonment and compensation of Rupees 2 lakhs will be fined. With an outlook of bringing it up to mark with advance democracies, this section got amended and introduction of more stringent provisions for pornography, and especially for child pornography.[25]

In present scenario of the section is such that, Section 67 of the Act deals with publishing of obscene information, 67A deals with publishing of sexually explicit/pornographic material and section 67B of the Act deals with child pornography.[26]



CHAPTER -3: INTELLECTUAL PROPERTY RIGHTS AND E-GOVERNANCE

In economic theory the property, is defined as a valuable resource and the way this resource is put to use id determined by an exclusive authority. It is evident that the ownership of property comes with a 'bundle of legal rights' i.e., the right of control over use of property, the right of ownership of property, right of excluding others from using the property, right to transfer, sell, lease or otherwise dispose of the property at owner's will. All

[23] Ibid.
[24] Ibid.
[25] Ibid.

[26] www.tutorialspoint.com (Dec. 11, 2021, 8:56 PM), https://www.tutorialspoint.com/information_security_cyber_law/offences_and_penalties.html.

this rights are collectively called property rights.

In virtual world framework, the objects existing are not of tangible nature like land, but are instead intangible in form of digital information. Example of digital information could be trade secrets, computer software, and literary works like articles, novels, journals, creative works like paintings, photographs and sound recordings etc., but being present on the digital realm they are at a risk of being exploited or embezzled. This implies that digital property are obliged to possess the property rights as well making their use and access restricted. Digital information, in terms of property, usually comprise of intellectual property, which is a creation of mind, such as inventions; literary and artistic works; and symbols, name and images used in commerce. [27]

The grant, protection and enforcement of intellectual property rights (IPRs) in cyberspace are governed by various national as well as international laws and treaties developed exclusively for intellectual property. The rights have been broadly classified by the world trade organization into Industrial property that consists of distinctive signs used to distinguish or identify an object, such as trademarks and geographical indications. Secondly, it consists of rights which encourage inventions, like patents, industrial designs and trade secrets.

The utilization of Information and Communication Technology (ICT) via government to facilitate or to provide government services, exchanging information, communication transactions and amalgamation of various standalone systems and services. [28]

CONCLUSION

The rate of cybercrime has increased to rate that can be considered as a worldwide epidemic. This issue is being tackled with the cyber security law prevailing all over the globe, different legal guidelines in association with cyber law have been passed by means of countries around the arena encompass digital signature legal guidelines as well as records technology legal guidelines. The cyber law also came into existence to create privacy. This is followed very genuinely in USA, legal guidelines which got used to establish this net privacy consist of following: Warren and Brandeis, Reasonable Expectation of Privacy Test, Privacy Act of 1974, foreign intelligence Surveillance Act of 1978, Homeland security Act, Gramm-Leach-Bliley Act, Intelligence Reform and Terrorism Act.

Cyber law has a tremendous rate of growth annually and this is only because of the growth in the cyber-crime rate. To face these cyber threats there are trends in cyber regulation. To recognize these issues is the top priority of government and cyber law organizations in near future. India for instance has funded cyber trend studies initiatives in each 2013 and 2014.India also held worldwide conference regarding cyber law in the year 2014. These efforts were made in the direction to promote cognitive

[27] ANIRUDH RASTOGI, CYBER LAW: LAW OF INFORMATION TECHNOLOGY AND INTERNET (1st ed. 2014).

[28] www.cyberjure.com (Dec. 11, 2021, 10:11 PM), http://www.cyberjure.com/ipr-in-cyberspace-h-4.html.

and international cooperation. It is also seen in India that the cyber courts are very less and the proper training to the police related to the cyber is proper. Due to this reason also the problem and the offences of cyber prevails.

BIBLIOGRAPHY

A) Books Referred

1. Albert J. Marcellai and Robert S. Greenfield in their book, Cyber Forensics-A Field Manual for Collecting, Examining and Processing Evidence of Computer Crimes (Aurebuch Publications, London, 2002).
2. Austin, Lecture on Jurisprudence: The Philosophy of Positive Law (J. Murray, London, 1st edn., 1920).
3. Bary C. Collin, The Future of Cyber Terrorism (University of Illinois, Chicago, 1996).
4. Chris Reed, Internet Law Text and Materials (Butterworths, London, 2000).
5. D. Thomas and B.D. Loader, Cyber-Crime Law Enforcement, Security and Surveillance in the Information Age, (Routledge Publications, London, 2000).

B) LIST OF JOURNALS & PERIODICALS REFERED

1. All India Reporter
2. Criminal Investigation Department Review
3. Criminal Law Journal
4. International Journal of Cyber Criminology
5. International Journal of Emerging Trend & Technology in Computer Science
6. International Journal of Engineering and Management Research

C) LIST OF REPORTS REFERED

1. National Crime Agency Reports
2. National Crime Records Bureau Reports
3. National Law Commission Report

*****