EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), ISSN: 2319-5045
Volume 5, Issue 2, July-December, 2016, Impact Factor: 4.189, Available online at: www.eduzonejournal.com

Cyber Laws in India - Critical Analysis

Minakshi Sharma

LL.M Scholar, Department of Law, Maharshi Dayanand University Rohtak

INTRODUCTION

The most significant of the numerous scientific and technological breakthroughs of this period was the marketing of the internet. The Indian market was inundated with mobile phones and computers. The proliferation of technology and the internet has led to a greater dependence of humans on these devices. The internet is now more interconnected with individuals than ever previously. A man can access the information he needs with a single click. Nevertheless, the prosperity of the web has also given rise to a multitude of unforeseen criminal activities. The progression of technological advances has led to the emergence of novel illicit activities and an increase in the scale and concentration of existing criminal activities. The field of Cyber Law primarily focuses on the various dimensions of the expanding body of technical knowledge. It establishes a collection of regulations pertaining to the issuance of licenses, license returns, and other matters concerning cutting-edge technologies such as computers, the internet, mobile devices, and others. Despite the fact that a significant portion of Indian cyber law addresses the risk of digitally produced offenses, cybercrime rates continue to rise incrementally.

What does the area of Cyber offence include?

According to Indian law, the precise definition of cyber offense is ambiguous. The Information Technology Act, 2000[1] or The Indian Penal Code, 1860[2] are the preeminent laws governing information technology and communication in India. Nevertheless, due to the vastness of the subject matter, precisely defining cybercrime is virtually unattainable. Perhaps the most prevalent definition of cybercrime is, "illicit activities in which the computer serves as either a tool or a target for both". Economic crimes, the trade in of illicit products, pornographic material, online wagering, intellectual property theft, email spoofing, forgery, online slander, and cyber harassment are all potential uses of the computer. Yet, the computer could potentially become the target of malicious activities such as data hijacking, email bombardment, data dosing, salami attacks, logic attacks, Trojan attacks, or physical damage to the system itself. This paper undertakes an examination of the various laws in place in India. Additionally, it aims to establish a framework for regulating unregulated cybercrimes in the country and examines the legal framework surrounding such offenses.

History of Cyber Crimes:

As a global wide area network, the Internet links computer systems from around the globe. The origins of the Internet can be traced back to 1960, while the United States funded research projects for its armed forces groups concerning the development of robust, fault-tolerant, and geographically dispersed networked computers. The aforementioned study brought to light the vast array of uses that computers have in virtually every aspect of contemporary human existence. In its entirety, the Internet experienced a phenomenal development between the years 2000 and 2009. Globally, the overall amount of Internet users increased from 394 million to 1,858 billion.[3]

Need for Cyber Laws:

Both offenses and people's reliance on digital technology are increasing in the twenty-first century. The primary purpose of the Internet was to facilitate the exchange of information and promote research. 'E-business,' 'e-commerce,' and 'e-governance,' among others, became increasingly prevalent as time passed. Cyber security regulations address all illicit activities carried out via the internet. The proliferation of online users has increased in tandem with technological progress, consequently generating significant pressure for stringent legislation and its enforcement. Cybercrimes affect every individual in the contemporary, highly computerized world. Previous technological barriers were overcome by the cyber change, which subsequently impacted every sector of the nation. To remedy this consequence, an appropriate legal framework guided by robust economic principles is necessary.

Laws Related to Cyber Crimes in India:

[1] Act No. 21 of 2000
[2] Act No. 45 of 1860
[3] Available at; https://blog.ipleaders.in/need-know-cyber-laws-india/

Similar to how the Information Technology Act, 2000 defines and addresses cybercrimes, it also imposes penalties on such offenses. The Indian Penal Code, 1860[4] governs all general offenses and is the foundational criminal code of India. The expansion of scientific encroachment has consequently led to a broader scope for these criminal activities. These transgressions can be easily categorized within the scope of the IT Act of 2000 and the IPC. As a consequence, cybercrimes in India are predominantly addressed through the subsequent two acts:

- Information Technology Act, 2000[5]
- Indian Penal Code, 1860[6]

➢ **Information Technology Act, 2000-**

At the turn of the 20th century, India recognized the information technology (IT) industry as the most important factor in achieving its goals of economic dominance and general progress. The broadening of IT education was a priority for both the central and state governments, which implemented mandatory fundamental computer training in government-affiliated institutions. Shortly thereafter, a significant portion of the populace acquired fundamental knowledge of computers. Investments in IT caused the nation's IT sector to flourish. The Information Technology Act of 2000 was enacted with two primary objectives in mind: to address the expanding demands of the IT sector within the nation and to identify and penalize individuals who engaged in its misuse.

The IT Act of 2000[7], specifically Chapter XI (S.65-S.78), addresses and deliberates on cyber offenses. In addition, punishments for the aforementioned offenses are specified. A limited number of criminal acts under the above mentioned act are outlined below:

- **interfering with computer source documents**: Section 65 of the "IT Act, 2000" establishes penalties for tampering with computer source documents, including "obstructing, destroying, or altering any data that is crucial to be maintained in compliance with the law." For instance, if a compact disc is presented in court and its parts are altered or a forged copy is produced, the offender faces a three-year prison term in addition to a fine.[8]
- **Identity Theft**: It refers to engaging in manipulative or deceptive activities via the aim to carry out an offense by utilizing the electronic signature, password, or any additional unique identification characteristic of another individual. The IT Act, 2000" stipulates that the perpetrator of the aforementioned offense is subject to a maximum incarceration sentence of three years and a fine of up to one lakh rupees. [9].
- **Cheating by personation by using computer source-** Individuals who engage in cheating by personation through a computer source are subject to a maximum prison sentence of three years and a fine of up to one lakh rupees, as stipulated by the IT Act of 2000.[10]
- **Privacy violation**: In a recent ruling, the apex court recognized and provided fresh interpretations regarding privacy breaches committed by prominent social media platforms such as Google and Facebook. The infringement of privacy was a subject of nationwide discourse prior to the aforementioned judgment being rendered. While section 66E of the IT Act, 2000 establishes penalties of imprisonment for three years and a fine of up to 2 lakh for similar offences, it has proven ineffective in establishing a limit on the infringement of individuals' personal data.
- **Punishment for Cyber Terrorism**: It is the use of the internet to extort or coerce others into committing violent acts that result in or threaten serious bodily harm or death, with the intention of achieving political or ideological objectives through intimidation or threat." Misuse of technology, including the introduction of viruses, malware, and the like, aids cyber militants; these activities have the potential to negatively impact society as a whole and even claim lives. Despite the fact that cyber terrorism is punishable by life in prison under section 66 F of the IT Act of 2000, this does not reduce the frequency of cyber terrorism attacks or the government's concern for the potential harm it may cause.
- **Spreading Obscene Matter**: The IT Act of 2000 punishes rigorously the dissemination of indecent material as a criminal offense. SEC 67 of the IT Act, 2000 stipulates that offenders may be sentenced to a maximum of three years in prison and a fine of five lakhs. Those who commit the same offence a second time may be sentenced to five years in prison and a fine of up to ten lakhs. The IPC also encompasses the sale, rental, or distribution of

[4] Act no 21 of 2000
[5] Act No 21 of 2000
[6] Act No 45 of 1860
[7] Act no 45 of 1860
[8] Bhim Sen Garg v. State of Rajasthan, 2006 Cri LJ 3463 Raj 2411;
[9] S.66C, Information Technology Act, 2000;
[10] S. 66D, Information Technology Act, 2000;

pornographic material in Sections 292 and 294. The defendant was judged guilty in Shivaprasad Sajjan v. State of Karnataka (2018) under section 67 of the "IT Act, 2000." The verdict was rendered in a legal proceeding involving a software engineer who had transmitted explicit emails and photographs to the victim from a café. Notably, the engineer resigned from his position and pursued an LL.B. in order to be prepared for any eventuality. The court has imposed a two-year prison term and a fine of Rs. 25,000.[11]

In addition, Section 67-B explicitly addresses the issue of child pornography, which is defined as the distribution of explicit content to individuals that are younger than 18 years old. As per the stipulations outlined in this part, initial offenders may face an aggregate prison sentence of five years and a monetary penalty of ten lakh rupees; consecutive criminals may be subject to a maximum prison term of seven years and a fine of ten lakh rupees.

- **Penalty and compensation for damage to computer, computer system, etc**.- Penalty and compensation for damage to computer, computer system, etc.—Section 43A of the IT Act, 2000 stipulates that in the event that an individual fails to protect sensitive personal data without the owner's or another person in charge of a computer, computer network, or computer system body corporate's authorization. The section requires the organization that manages personal information to consent to technical safety steps and procedures to prevent abuse of data.
  Furthermore, the IT Act of 2000 confers authority upon the federal government to establish safety protocols and guidelines, as well as issue governing principles, in order to prevent violations of the law. Additionally, the Act grants the legislature authority to execute and enact laws more effectively.

➢ **Indian Penal Code, 1860:**

In consideration of the IT Act of 2000, the Indian Penal Code, 1860 was amended in 2010 to include electronic documentation and records as evidence. Therefore, the IPC criminalizes offenses associated with the fabrication of authentic documents and the creation of fraudulent documents. The 2010 Amendment amended the sections pertaining to "forged entry in any record" and "forged document," including S-192, S-204, S-463, S-464, S-464, S-468 to S-470, S-471, S-474, and S-476, among others. With the exception of these two statutes, laws such as "The Evidence Act, 1872" contain limited provisions addressing the liability of cyber threats. However, a significant portion of the framework for the implementation of Indian law concerning cybercrimes is established by these two legislation.

CRITICAL ANALYSIS

Crimes mirror the ever-changing nature of society; advancements in technology and educational systems have also contributed significantly to the progression of criminal activities. Over time, new offenses have emerged, which has had a pervasive impact on the general populace. Furthermore, contemporary criminal activities are executed in extraordinary ways possible due to the utilization of cutting-edge technology. The Information Technology Act, which was enacted in 2000 and amended in 2008, was designed to regulate cybercrime in India. However, twenty years later, the IT Act still faces numerous obstacles as a result of the rapid development of technology. Although the act has been successful in establishing a framework of regulations in the digital realm and addresses a limited number of pressing issues related to technology exploitation, it also possesses significant limitations. There remains a list of offenses that, due to the lack of stringent penalties or sanctions, encourage offenders to exploit the computer-generated environment. Certain aspects of cyber legislation necessitate careful consideration. e.g.-Spam is an abbreviation for unwanted bulk email. Spam is an extremely prevalent issue today. With all due respect, the IT Act of 2000 makes no mention whatsoever of the issue of spamming.

Phishing, an illicit fraud technique, involves the attempt to acquire confidential data, including but not limited to user names, passwords, and card details. It serves as an example of the "social engineering" technique utilized to mislead users. Phishing is not explicitly addressed in the "Information Technology Act, 2000"; the term "cheating" is used to refer to it in the IPC.

Data security in Internet Banking- The primary objective of data protection regulations is to safeguard the interests of individuals whose information is under the management and processing of third parties. While the IT Act of 2000 addresses unauthorized access, it contains no provision concerning the integrity of customer transactions. The provisions of this act absolve banks of any obligation to safeguard their clients' information. In India, the accountability of institutions is determined solely by agreement, as Indian law contains no specific legislation pertaining to this matter.

[11] https://thelogicalindian.com/news/cyber-crime-conviction-karnatka/

Privacy Protection-Legislation pertaining to the expanding domain of cyberspace is a constant source of novel regulations enacted by the parliament, whereas the "IT Act, 2000" adequately delineates common cyber offenses. "Privacy, in its most fundamental form, grants each individual the ability to exist independently within an impregnable core." The protection of data and personal information is crucial due to the immense importance that information and technology hold in private, professional, and commercial spheres. An additional noteworthy aspect that warrants attention is that India has lost out on numerous lucrative foreign investments and industrial prospects due to the absence of a comprehensive privacy legislation. The expansion of the electronic commerce industry in India has been adversely impacted by this deficiency. Therefore, an act addressing the various privacy-related issues is an absolute necessity in the present day. In the event that a comprehensive legislation cannot be enacted, it is advisable to incorporate rigorous provisions pertaining to "privacy and data security" into the existing acts..

Cyber War- Equally absent from the cyber laws was the concept of "cyber war." India has been the target of numerous cyberattacks launched by foreign nations in the modern era. Certain classified information was supplied to the culpable individuals as intelligence during the 26/11 attacks. Online platforms are not subject to specific regulations regarding the preservation of domain names, despite the fact that trademark and copyright violations do occur there. Certainly, the legislature does not consider this particular aspect. The act continued to be ineffective in containing cybercrimes that transcended geographical boundaries.

The legislation contained within "The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011" serves to standardize the country's existing data protection system. Rule 8(1) pertains to the necessity for the implementation of logical safety measures and procedures. With respect to the privacy concern raised in "Aadhar violating Right to Privacy," the legislation concerning the confidentiality of data underwent another revision on May 4th, 2017. Document "Guidelines for Securing Identity Information and Sensitive Personal Data or Information in Compliance with the AADHAR Act, 2012 and the Information Technology Act, 2000" was issued by the Ministry of Information Technology of the Government of India. "The B.N. Shrikrishna Committee" reexamined the world of various authorities in broad terms in the context of "data protection" and the "Right to Privacy" and issued a report that served as the basis for the new "Right to Privacy Bill, 2017."
„[12] „.[13]

CONCLUSION AND SUGGESTIONS:

However, the concept of a society devoid of crime is purely fictitious. This is especially true for societies situated in developing nations that rely heavily on technology. Cybercrimes are on the rise, and legislators must exert considerable effort to stop them. There are two facets to technology: it has both positive and negative effects. Steganography, Trojan horses, scavenging, and similar activities, while technological in nature and not inherently criminal, are classified as "cyber crimes" due to their malicious intent. As a result, it is incumbent upon legislators to ensure that the advancement of science and technology is conducted in a morally upright and lawful manner, rather than for criminal purposes. A few recommendations for enhancement are as follows:

The "IT (Amendment) Act, 2008" reduced the severity of penalties for the majority of offenses. severe consequences ought to be enforced on the offender. It is necessary to render non-bailable the majority of cyber offenses in order to instill fear among the public. Merely establishing rules and regulations will not effectively impede criminal activity. The primary responsibility for ensuring compliance with relevant legislation is for the three stakeholders to increase their awareness regarding cybercrimes. Stakeholders can be categorized into the following groups: users; Online or network service providers, banks, and other intermediaries; and sovereigns, regulators, legislators, and officials.

1. To safeguard the confidentiality of individuals and organizations, meticulous legal management is necessary.
2. "Cyber war" should be classified as a criminal offense according to the IT Act, carrying a more severe penalty.
3. The provisions outlined in "section 66A" of the "IT Act, 2000" do not violate reasonable limitations placed on the "right to freedom of speech and expression" as protected in Article 19 of the Indian Constitution. This flaw must be rectified in order for the stipulations to be legally acceptable.

[12] G.S.R. 313(E) Ministry of Communications and Information Technology (Department of Information Technology) Notification, New Delhi, (Apr.11, 2011).
[13] B.N. Shrikrishna J., White Paper of the Committee of Experts on a Data Protection Framework for India, Ministry of Electronics and Information Technology, (2017)

4. Cybercrime is best constrained through public education and awareness regarding cyberspace. Ignorance of one's rights and legal obligations may even impede progress and have an impact on the administration of justice.
5. Irradiation and the reduction of cybercrimes may benefit from the arrangement of a parliamentary management body in accordance with the requirements for preciseness and precision in duties.
6. Effective public awareness and constructive governmental collaboration can be facilitated through the provision of suitable education to various government agencies and legal authorities tasked with implementing cybercrime cases, as well as the organization of diverse awareness programs.

REFERENCES

[1]. Indian Penal Code, 1860;
[2]. Information Technology Act, 2000;
[3]. Code of Criminal Procedure, 1973;
[4]. Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1;
[5]. www.tigweb.org/actiontools/projects/download/4926.doc;
[6]. https://www.tutorialspoint.com/information_security_ cyber_law/introduction.htm;
[7]. https://www.slideshare.net/bharadwajchetan/anintroduction-to-cyber-law-it-act-2000-india;
[8]. http://www.academia.edu/7781826/IMPACT_OF_SOCI AL_MEDIA_ON_SOCIETY_and_CYBER_LAW ;
[9]. http://searchsecurity.techtarget.com/definition/emailspoofing;
[10]. https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf;
[11]. https://blog.lawskills.in/2019/02/15/critical-analysis-of-the-laws-against-cyber-crimes-in-india/;
[12]. http://www.helplinelaw.com/employment-criminaland-labour/CDII/cyber-defamation-in-india.html;
[13]. http://ccasociety.com/what-is-irc-crime/;
[14]. http://searchsecurity.techtarget.com/definition/denialof-service;
[15]. https://www.irjet.net/archives/V4/i6/IRJET-V4I6303.pdf;
[16]. http://niiconsulting.com/checkmate/2014/06/it-act2000-penalties-offences-with-case-studies/;
[17]. http://www.cyberlawsindia.net/cyber-india.html;
[18]. https://en.wikipedia.org/wiki/Information_Technolo gy_Act,_2000;
[19]. https://www.ijarcsse.com/docs/papers/Volume_5/8_ August2015/V5I8-0156.pdf;
[20]. https://cybercrime.org.za/definition
[21]. http://vikaspedia.in/education/Digital%20Litercy/inf ormation-security/cyber-laws;