

CYBER LAWS IN INDIA: A CRITICAL ANALYSIS

Dr. Pratima Devi

Assistant Professor, Department of Law, MDU, Rohtak, Haryana

ABSTRACT

With omnipresent technology and the network; the dependency of human being over these gadgets increased day by day. Today, the Indian markets are flooded by computers and cellular phones and the internet has joined the people like never before. Information required by a man is just one click away from him. On the other hand, the internet's success has also resulted in numerous unanticipated offences. The advancement in the technology gave birth to new-fangled wrongs and the enlargement in the enormity and concentration of the present crimes. Aura of Cyber law is mainly concerned with the different facets of the growing technical knowledge. It grants the set of laws relatable to the granting licenses, return of licenses & other conducts concerning computers, internet, mobiles and other advanced technologies. Though, the big part of the Indian cyber law deals with the threat of computer-generated crimes, still the crime rates in cyber field is increasing gradually. .” In the present paper, an attempt is made to analyze the different laws situated in India; it also projected to ensure the uncontrolled cyber-crimes in India, and the legal regime around cyber-crimes is done.

Keywords: Information, cyber, Internet, data, Computer.

INTRODUCTION

There is no exact meaning of cyber offence under Indian law. The Indian Penal Code, 1860 and The Information Technology Act, 2000 which are the leading law in India for Information Technology and communication did not define the term Cyber-crime. Though, the area of the crimes is that much wide; that defining the cyber crime is next to impossible. The most common definition of Cyber crime maybe, “*the unlawful acts wherein the computer is either a tool or target both*”. The computer maybe used in the- “financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, email spoofing, forgery, pornography, cyber defamation, cyber stalking. The computer however maybe target for the unlawful acts in the cases like- data theft, email bombing, data didling, salami attacks, logic attacks, logic bombs, Trojan attacks, physically damaging the computer system.”¹

History of Cyber Crimes

“The Internet is a global wide area network that connects computer systems across the world.”² The beginning of the Internet can be derived to the time in 1960 when the US decided to finance the research assignment of its armed forces organizations to construct strong, fault tolerant & distributed computer based networks. The above study popularized the immense applications of computers in approximately every phase of present human life. Overall, the remarkable expansion in the Internet was seen from the year 2000 to 2009. The number of Internet customer world widely arose from 394 million to 1.858 billion.³

Need for Cyber Laws

¹ Monika Bhardwaj, Cyber Crime; retrieved from <http://EzineArticle.com/3479824>.

² <https://en.m.wikipedia.org/wiki/internet>

³ <https://blog.ipleaders.in/need-know-cyber-laws-india/>

In the 21st century, the humanity is becoming to a greater extent digitally dependent and so are the crimes. Internet was originally come into existence for study and information circulation device. With the passage of time, it happened to more common with “e-business”, “e-commerce”, “e-governance” etc. All the unlawful acts committed by internet are dealt by cyber laws. As with the advancement in technology, internet users are rising day by day, the requirement for strong laws and their submission too assembled immense drive. Today, when the world is highly digitalized, everyone is affected by cyber crimes. The cyber revolution unlocked the earlier technologies, which had a trickledown effect on every sector of country. A suitable lawful management with strong socio-economic template is required to cure such effect.

LAWS RELATED TO CYBER CRIMES IN INDIA

As, crimes related to cyber are defined and discussed under the “Information Technology Act, 2000” the act also penalizes cyber crimes. “The Indian Penal Code, 1860” is the fundamental criminal law in India, which deals with all the general offences. As, with the encroachment in science, the scope of these crimes is has also become wider. These offences can simply be classified under the ambit of IPC as well as IT Act, 2000. Therefore, in India, the cyber crimes are mainly dealt in the following two acts:-

- “Information Technology Act, 2000(21 of 2000)”.
- “Indian Penal Code, 1860 (45 of 1860)”.

➤ **“Information Technology Act, 2000”**

India in the beginning of 20th century had acknowledged IT sector as the primary factor in seeking to accomplish its dream of becoming economic power and overall development. The government at the centre as well as state level took initiative for the expansion of IT teaching, basic computer education were made compulsory in the government affiliated schools. As a result a large area of population was soon aware about the basic computer skills. The investment made in the IT boomed the IT industry in the country. The Information Technology Act, 2000 was designed both to furnish the growing needs of the IT community in the country and to recognize and punish those who indulged in misusing it.

Chapter XI (S.65- S.78) under the IT Act, 2000 deals and discusses the cyber offences. It also stipulates the penalties for the above stated offences. Few offences which are punishable according to the “IT Act, 2000” are discussed as follows:-

- **interfering with computer source documents:** Section 65 of the “IT Act, 2000” lay down sentence for, “hiding, demolishing & changing any data which is essential to be preserved in accordance with the law; e.g., if a compact disk is submitted before a court, alteration in its contents or the production of a fabricated copy is punishable with 3 year imprisonment with a fine.”⁴
- **Identity Theft:** It means the do something deceitfully or fraudulently by use of the e-signature, password or any or any other unique identification feature of any other person with the intention of committing the wrong. According to “IT Act, 2000” the offender committing the abovesaid offence is liable for imprisonment upto 3 years and fine which may extend to 1 lakh ⁵.

⁴ Bhim Sen Garg v. State of Rajasthan, 2006 Cri LJ 3463 Raj 2411;

⁵ S.66C, Information Technology Act, 2000;

- **Cheating by personation by using computer source.**—: The IT Act, 2000 punishes those who commit “cheating by personation” via a computer source with imprisonment upto 3 year and fine which may extend to 1 lakh.⁶
- **Privacy violation:** The apex court in the very recent judgment⁷, acknowledges and gave new interpretations about breach of privacy by popular social cites like, ‘Google & FB’. The Privacy violation was a topic of national debate before pronouncement of the above mentioned judgment. Although, The IT Act, 2000 set downs imprisonment for 3 yrs and fine upto 2 lakh for the same u/s 66E, but it didn’t help in putting limit on infringing personal data of people.
- **Punishment for Cyber Terrorism:** “It is use of internet to conduct violent acts that results in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation”⁸. The abuse of technology such as introducing virus, worms etc. assist the cyber terrorists, these actions lean to have an effect on the life of the public in adverse manner and can even result in the loss of lives of people. However, The IT Act, 2000 under section 66 F has made the cyber terrorism rigorously punishable with life imprisonment, but it neither lowers down the rate of incidents of cyber terrorism attacks nor government’s concern about potential damage that could be caused by it.
- **Spreading obscene matter:** Broadcasting obscene substance is a strictly punishable offence under the IT Act, 2000. According to S 67 of IT Act, 2000 punishment amount up to 3years with fine 5 lakhs can be imposed on the offender; and the second time offender can be awarded the punishment for five years & a fine up to 10 lakh. Sections 292 & 294 of IPC also contemplates the selling, hiring or distribution of pornographic matter. In Shivaprasad Sajjan v. State of Karnataka (2018), the offender was found guilty under section 67 of “IT Act, 2000.” The judgment was delivered in a case where a software engineer who had sent obscene emails and photographs from a café to victim. Interestingly, the engineer quit his job and completed LL.B, so that he could defend himself in case. The court has sentenced him imprisonment of 2 years and 25000/- fine.⁹

Moreover, Section 67-B absolutely deals with the child pornography i.e spreading obscene material to those who are below the age of 18 years. According to provisions of this section the first time offenders are punishment imprisonment upto 5 years and fine of 10 lakh, a subsequent offender can be sentenced upto 7 years imprisonment and fine of 10 lakh.

- **Penalty and compensation for damage to computer, computer system, etc.-** According to section 43A of the IT Act, 2000 the where any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network body corporate fails to protect sensitive personal data. The company operating the private data is needed in the section to agree to rational security measures and practices to avoid the misuse of data.

⁶ S. 66D, Information Technology Act, 2000;

⁷ K.S. Puttaswamy v. Union of India, 2017 10 SCC 1;

⁸ <https://en.m.wikipedia.org/wiki/Cyberterrorism>;

⁹ <https://thelocalindian.com/news/cyber-crime-conviction-karnatka/>

The IT Act, 2000; in addition empowers the central government to issue guiding principles & set down the safety measures & practice to make certain that, the breach of law does not take place. The Act also empowers the legislature for better execution and the enactment of law.

➤ **“Indian Penal Code, 1860”**

After the 2010 amendment in Indian Penal Code, 1860 in light of the IT Act, 2000; electronic records and electronic documents under the domain of evidences. Therefore, the offences related to the making of false documents and fabricating the original documents is made punishable under IPC.

The Sections related to ‘forged entry in any record’ or ‘forged document’ e.g. S-192, S-204, S-463, S-464, S-466, S-468 to S-470, S-471, S-474 & S-476 and so on, have been amend by the 2010 Amendment.

Except these two statutes, other legislations like “The Evidence Act, 1872” also have few provisions which deal with culpability of cyber threats. But, the basic outline for the enforcement of Indian law adjacent to cyber-crimes is substantial deal by of these two statutes.

CRITICAL ANALYSIS

Crimes are as dynamic as a society is; with the substantial development in educational system and up gradation of the technology in the society, the criminal have progressed too. New offences have originated with the time and it affected the people at large. In addition, the common crimes are done today with extraordinary exceptional ways with the help of advanced technology.

IT Act was passed in the year 2000 and subsequently amended in the year 2008 to control cyber crimes in India. Though, even after 20 years there are a lot of challenges before the IT, Act due to fast growth of technology. Whereas, the act has proved victorious in providing the construction of set of laws in cyber world and deals with a small quantity of urgent concerns of abuse of technology, it also has severe drawbacks. A list of offences is still there which because of absence of strict penalties or sanctions prompts the perpetrators to abuse the computer-generated space. Some areas of cyber laws require attention. E.g.-

Spam- spam means, unsolicited Bulk E-mail. Spamming is very common problem today. But the IT Act, 2000 does not talk about the problem of spamming by any means.

Phishing- Phishing is the illegally deception procedure of trying to obtain sensitive personal details such as user names, passwords, & cards information. It is an illustration of ‘social engineering’ procedure bring into play to deceive users. There is no legal provision adjacent to phishing in the “Information Technology Act, 2000”; throughout the IPC have its mention in form of ‘cheating’.

Data security in Internet Banking- The regulations related to Data protection first & foremost aims to preserve the interest of people whose information is managed and processed by others. The IT Act, 2000 discuss about unlawful access, but it does not have any provision related to maintaining the reliability of customer’s transactions. According to the provisions of this act, no duty is of banks to guard the information of its clients. In India, the banks accountability would come up because of agreement only, as no specific law is present in Indian Law related to this point.

Privacy Protection- Whereas the ordinary cyber offences are sufficiently described under the “IT Act, 2000”; the parliament continuously keeps making new-fangled regulations to control the widening area of the cyber world. “Privacy, in its simplest sense, allows each human being to be left alone in a core which is inviolable”.¹⁰ Safety of data & personal information are important matters as information and technology believes immense significance in private, professional and commercial areas. Another important thing which we need to make a note upon is that because of nonexistence of a precise privacy law in India, many important foreign investments and other industrial opportunities has slipped from the hands of our country. Because of this insufficiency the actual growth of electronic business in India has also affected. Therefore, an act to tackle the different problems related to privacy is utmost need of today. If it is not possible to bring a complete act, then at least some strict provisions dealing with “privacy and data security” should be introduced in the present acts.

Cyber War- The issue of ‘cyber war’ too didn’t find any place in the cyber laws. In the modern time, India has witnessed a number of cyber assaults from foreign countries. ‘In the 26/11 attacks, a number of classified data were provided as Intel to the perpetrators liable for liable for their actions’.¹¹ The Trademark and copyright infringements do take place on the internet; however there is no specific enactment for the protection domain names on the net. This side is totally not taken into account by the legislature. Where cyber crimes came with no territorial boundaries the act remained a failure to rein those attacks.

The set of laws in “The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011”¹² harmonize the present data safety system in the nation. Rule no. 8(1),¹³ discuss regarding the requirement intended for the subsistence of rational safety measures & methods. In the light of the question of the privacy “Aadhar infringing Right to Privacy, the law pertaining to data privacy” was again revised and on May 4th, 2017. The Government of India (department of Ministry of Information Technology), published “Guidelines for Securing Identity Information and Sensitive Personal Data or Information in compliance with AADHAR Act,2012 and the Information Technology Act,2000”.¹⁴ “**The B. N. Shrikrishna Committee**” again examined the different authorities’ world widely in the luminosity of the “Right to Privacy”, “data protection” and presented a report which gave a foundation for the new “Right to Privacy Bill, 2017”.¹⁵

SUGGESTIONS

Few suggestions for improvement are as follows:

1. The “IT (Amendment) Act, 2008” lower down the amount of penalty for the most of the offences. There should be strict penalties imposed in the offender.

¹⁰ Kharak Singh v. state of UP & others; 1962 (1) SCR 332

¹¹ Ijlees.kypublications.com

¹² G.S.R. 313(E) Ministry of Communications and Information Technology (Department of Information Technology) Notification, New Delhi, (Apr.11, 2011).

¹³ IT Rules, 2011, Rule 8(1).

¹⁴ K.S. Puttaswamy v. Union of India, 2017 10 SCC 1;

¹⁵ 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)

2. The most of the cyber offences need to be made non-bailable offences, so that there can be fear among people.
3. Only making the rules and regulations will not stop commission of crime. For the proper execution of the concerned laws; the primary duty lies on the three stake holders to get more alert about the cyber crimes. These stake holders can be classified as follows:
 - the sovereigns, supervisors, lawmakers & representatives;
 - Internet or Network Service providers or bank and other intercessors; and
 - The users.
4. Detailed legal administration is required to defend the privacy of people and organizations.
5. 'Cyber war' should be made an offence under the IT Act and higher punishment should also be there for this offence.
6. The components of "section 66A" of the "IT Act, 2000" does not fall under reasonable restrictions imposed on the 'right to freedom of speech and expression' under the article 19 of constitution of India. This defect required to be removed to make the provisions lawfully maintainable.
7. The limit on cyber crimes can be put only by awareness and cyber learning across the public. The lack of alertness about the rights and laws can even result in slow down the growth and affect the justice delivering system.
8. The configuration of a legislative managerial body to meet the accurateness and precision in duties can prove to be of good impact for irradiation and decrease of Cyber Crimes.
9. The appropriate education to the different administrative powers and legal authorities for putting into effect the cases interrelated to Cyber Crimes and association of diverse alertness camps by government can be helpful and productive for the general public and its growth in a positive manner.

CONCLUSION

Although, a society without a crime exists only in imaginations. Particularly in a society which falls in list of developing countries and which is more dependent upon technology. Cyber-crimes are increasing day by day and the law makers have to go a long way to control them. Technology has two aspects; it has both good as well as bad impact. Steganography, Trojan horse, Scavenging etc. are all technology and not crimes per se, but with an illicit intent they fall in the range of 'cyber crimes'. Accordingly, it is the responsibility of lawmakers to make certain that science and technology develops in a hale and hearty manner, and is exercised for lawful and decent business expansion and not for committing crimes.

REFERENCES

- Information Technology Act, 2000;
- Code of Criminal Procedure, 1973;
- Journal of Alternative Perspectives in the Social Sciences (2011) Vol 3, No 1;
- www.tigweb.org/actiontools/projects/download/4926.doc;
- https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm;
- <https://www.slideshare.net/bharadwajchetan/anintroduction-to-cyber-law-it-act-2000-india>;
- http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW ;

- <http://searchsecurity.techtarget.com/definition/emailspoofing>;
- https://www.ijarcse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf;
- <https://blog.lawskills.in/2019/02/15/critical-analysis-of-the-laws-against-cyber-crimes-in-india/>;
- <http://www.helplinelaw.com/employment-criminaland-labour/CDII/cyber-defamation-in-india.html>;
- <http://ccasociety.com/what-is-irc-crime/>;
- <http://searchsecurity.techtarget.com/definition/denialof-service>;
- <https://www.irjet.net/archives/V4/i6/IRJET-V4I6303.pdf>;
- <http://niiconsulting.com/checkmate/2014/06/it-act2000-penalties-offences-with-case-studies/>;
- <http://www.cyberlawsindia.net/cyber-india.html>;
- https://en.wikipedia.org/wiki/Information_Technology_Act,_2000;
- https://www.ijarcse.com/docs/papers/Volume_5/8_August2015/V5I8-0156.pdf;
- <https://cybercrime.org.za/definition>
- <http://vikaspedia.in/education/Digital%20Literacy/information-security/cyber-laws>