IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER CRIMES AND INFORMATION & TECHNOLOGY ACT IN INDIA

*Priyanka Verma

***ABSTRACT**: The new boon brought by information technology has brought its scar in the form of cybercrime. To address this issue the United Nation through its core agency, United Nations Commission on International Trade Law (UNCITRAL) had formulated model legislation on electronic commerce. The Information Technology Act, 2000, is the prime legislation dealing with cyber offenses in India, which is based on the United Nations Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL). The Information Technology Act, 2000, is applicable to the whole of India, including any offense committed outside India, if such contravention involves a computer, computer system or computer network located in India. This instant paper has been written in order to evaluate that whether this Act has been dealing with every cyber crime, offence or contravention which is necessary to be dealt with, in today's scenario. Moreover, the provisions of the Act has been analyzed which are dealing with the cyber offences or contraventions. Further, an attempt has been made to discover the grey areas of the Information and Technology Act, 2000; along with certain suggestions.*

INTRODUCTION: The concept of crime is not a modern one but it has been existing from time immemorial. However, time to time, the concept and nature of crimes have changed. In addition, the definition of crimes has been changed accordingly.[1] The purpose of the law is to regulate the laws. Law plays an important role in dealing with the traditional offences. Due to the advancement of technology, we don't know properly what will be the situations which the law should cover, especially for the cyber crimes, because the cyber crimes are not properly discovered nor there are some certain ways by which we can define the cyber crimes in a certain way. The cyber crimes are increasing day by day without and hurdle. There has been number of cyber offences emerging, which are not having definite law to be dealt with. In the era of digitalization, privatization and globalization, where the world is one by connecting to each other by the computers, etc; but unluckily there is no proper law prevailing which would deals

*Research Scholar, UILS, Chandigarh University, Gharuan, Punjab.

[1] The Law Relating To Cyber Crime In India, *available at:* https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08_chapter%203.pdf (last visited on March 8, 2020).

with each and every cyber crime & offences. Taking into consideration the concept of cyber crime, the law and the judicial approach towards it, the system is very much week in its nature. Though some of the traditional crimes, in present scenario, can be committed online; but there are certain distinctions between the traditional and cyber crimes. Some of them are:

- Awareness: In traditional crimes, there is proper awareness regarding it, i.e., people know this is wrong or this is right and this would lead to these consequences; while in cyber offences and crimes, there is no such kind of awareness among the people. The lack of proper awareness regarding the cyber offences and crimes are the boost for some of the online offenders to commit crimes fearlessly and without any kind of disturbances.
- Tackling: The traditional crimes are little bit easier to tackle as compared to the cyber crimes, because for the cyber crimes and offences, there is no specific or certain law which provides that how these crimes can be prevented or controlled. Thus, the tacking procedure in respect of traditional and cyber crimes are different and somewhere its very much complicated regarding the cyber crimes and offences.
- Prove: The traditional crimes are not that much difficult to prove as the cyber crimes offences are, in reality; because we can prove the traditional crimes by just proving that the requirements or conditions necessary for constituting a crime are there in a specific or a particular offence or crime, but in the cyber crimes, there is no such invention or discovery of adequate techniques by which we can prove a case beyond a reasonable doubt.
- Nature: The traditional crimes are definite in nature, i.e., it's pretty much clear that this would amount of this and that, like killing of a man would amount to murder of a person; whereas the cyber crimes are not yet properly discovered and thus, we cannot find the proper nature of any of cyber crime or offences. Therefore, the traditional crimes are quite simple while the cyber crimes are tricky and complex in its nature.
- Detection: The person who has committed the traditional crimes are little bit easier to detect as compared to the cyber crimes, because of the availability and discovered techniques in respect of traditional crimes, while on the other hand the detection process has not been properly invented.
- Boundary: In traditional crimes, there is physical boundary or restrictions somewhere, while in cyber crimes, there are no such territorial restrictions. The offender or the wrongdoer indulging in cyber crimes can do any wrong by being within the territories of India or outside the territories of India. Many of the crimes has been planned by the online system outside the limits of the
- Examples: The traditional crime's examples may be theft, murder, dacoity, robbery, etc, which have been provided either in Indian Penal Code, 1860, or in any other specific law on any subject for the time being in force in India. And the examples of cyber crimes are hacking, phishing, cyber fraud, etc., and some of them are yet not discovered, because due to the vastness in the communication and technology and its increasing works through online and digital platforms, it is not easy to discover all of the cyber crimes and offences.
- Frequency: In traditional crimes, the frequency of crime is far more less as compared to the cyber crimes and offences. The traditional crimes can be committed against a person, two person or more than that, but the cyber crimes can be committed against the number of persons by just using the computer system by being at home even.

- Essentials: As far as the essential of the any crime are considered, there are two essentials, i.e., the actus reus and the mens rea. That means the act must have been occurred and there should be the intention or the guilty mind of the person committing the act. In the traditional crimes, there is difficulty in proving the mens rea of an offence, and the actus reus can be proved by the act of the person itself. Thus, in the traditional crimes, we have to assume the mens rea from the conduct, or guilt of the accused, or from the series of the circumstances in a particular case before the Court. But in case of cyber crimes, it is the actus reus which is difficult to prove, because the mens rea could be inferred from the illegal access of the accused. Thus, mens rea is far easy to be proved in cyber crimes as compared to the traditional crimes and hence the easy and difficult essentials of both of them are opposite to each other.
- Target: In traditional crimes, the target can be one or more, which can be discovered; while in cyber crimes, the target can't be detected. Thus, the victimization in the cyber crimes is on the larger level.
- Jurisdiction: In traditional crimes, the jurisdictional issues is not much complex, if we compared it with the cyber crimes.
- Punishment: The punishment of the traditional crimes is definite and proper laws are also there in order to deal with them like in Indian Penal Code, 1860, there has been specific punishment prescribed for the offences; but in case of cyber crimes, there is no such particular law on cyber crimes which deals with each and every kind of cyber crimes.

INFORMATION & TECHNOLOGY ACT, 2000: The cyber crimes are the computer oriented crimes. Although there is no proper law to deal with the cyber crimes in India, but there is Information Technology Act, 2000; which deals with some of the issues coming under the cyber crimes. The Information Technology Act, 2000; is not as such talking about the cyber crimes. It was basically passed to encouraged International trade and economy of different countries. It is a wide Act, which not only dealing with the computer, computer system; but also deals with every information through any technology which connected us with the e-commerce. Information Technology Act, generally deals with the civil wrongs, but somewhere also deals the penal provisions also. Section 43, 43A, 46, 47, and 65 to 74 deals basically with the cyber crimes.

1. SECTION 43: It talks about penalty and compensation to the person whose computer, computer system or computer network has been accessed or secured by the unauthorized access. If any person without the permission or consent of the owner,

a) accesses the computer,

b) downloads, or make copies or extracts

c) introduces or causes to introduces any contaminant or virus in the system which results in hacking, cracking, blending or blacking of the system,

d) damages, or causes to damages any computer, computer system or computer network (it can be a part of data leakage, or cracking),

e) denial to any access to the system,

g) provides any assistance or abets or gives tutoring to have an unauthorized access to the computer of any other person,

h) charges the services availed by any another for unauthorized access,

i) deletes the information, diminishes or destroying, or altering its value,

j) steals, conceals, etc. any information

shall be liable to pay damages by way of compensation by the accused to the victim.[2]

It covers the cases of cracking, computer trespass, data theft, privacy violation, software privacy or theft; digital copying, data and computer database theft; deletion, alteration, damage, modification of stored computer data or computer programs leading to data interferences; computer or online fraud, forgery; spamming; cases of system interference or computer devices; illegal access, misuse of computer devices; phishing, theft of identity devices; hacking, denial of service attacks; cases of computer programme or software's copyright violation, etc.[3]

2. SECTION 43A: It lays down that where a person has fails to protect the sensitive personal data or information, i.e., where anyone is negligent in operating and causing wrongful gain to any other person, etc. shall be liable to a punishment of 3 years or compensation up to 5 lakhs or both.

3. SECTION 47: It deals with the quantum of the compensation. The adjudicating officer has to see the amount of gain or unfair advantage, the amount of loss caused, and its repetitive nature (if there), and shall be punished accordingly.[4]

4. Some cyber offences as per Information and Technology Act, 2000:

- SECTION 65: It deals with the tampering with computer source documents- Punishment up to 2 years, or compensation up to 2 lakhs or both. It is the discretion of the Court to decide. The offences like hacking or cracking comes under this.
- SECTION 66: It deals with computer related offences- Punishment up to 3 years and compensation up to 5 lakhs or both.[5] For subsequent offenders, up to 5 years or 10 lakhs or both. [6]
- SECTION 66A: Any person who is sending to any other person, using communication, any information which grossly offensive, menacing, or destructive, which a person known to be false or untrue and that causes hurt, enmity, hatred, injury, insult, tarnishes image, ill-will, i.e. with evil intention; by e-mails or by any other kind of electronic messages; is liable to punishment up to 3 years or with fine or both. In this particular section, fine is not limited and it is totally upon the discretion of the Court to decide upon, after seeing the

[2] Information and Technology Act, 2000.
[3] Dr. Jyoti Rattan, *Cyber Laws & Information Tecghnology* 273-77 (Bharat Law House, New Delhi, 6th edn., 2017).
[4] *Supra* note 2.
[5] *Ibid.*
[6] Information and Technology (Amendment) Act, 2008.

specific facts and circumstances of the case. The cyber stalking, cyber harassment, cyber sexual harassment, outraging the modesty, etc., comes under this. Section 66A is to be read with Section 67, 67A of the Act.

- SECTION 66B: It lays down that whoever dishonestly deceives or retains any stolen computer resource or device, is liable to be punished for a term which may extend up to 3 years or fine up to 1 lakh or both.[7] Theft, and piracy offences are covered under this.
- SECTION 66C: It deals with the identity theft. Punishment up to 3 years or fine up to 1 lakh or both.[8]
- SECTION 66D: It deals with punishment for cheating by personation by using any computer resource and is liable is be imprisoned which may extend up to 3 year or fine up to 1 lakh or both.[9]
- SECTION 66E: It lays down the punishment for the violation of privacy, i.e., up to 3 years or up to 2 lakhs fine, or both. [10]
- SECTION 66F: Punishment for cyber terrorism- up to life imprisonment.[11]
- SECTION 67: Section 66 is a generalized section and includes many acts which injures and harms anyone. But Section 67 specifically provides for the punishment for publishing any obscenity images, material, etc., in any electronic form. Its punishment is up to 3 years or with fine up to 5 lakhs or both. In case of subsequent event, it may extend up to 5 years or up to 10 lakhs or both.[12]
- SECTION 67A: It lays down the punishment for publishing or transmitting any material which contains sexually explicit act or conduct, in electronic form; shall be liable to be punished for an imprisonment up to 5 years or with fine 10 lakhs or both. In case of subsequent event, it may extend up to 7 years or 10 lakhs or both. [13] In case of incapacity to pay fine, the more punishment can be given by the Court to decide what the amount of fine and how much the punishment is proper for the justice after considering the facts and circumstances of the case in hand.
- SECTION 67B: It provides for the punishment for publishing or transmitting any material which depicts children in sexual exploits acts in any electronic form, for which the punishment is same as provided under section 67A. This law needs to be reformed by amending the punishment under this section. The children are the future of the nation. The punishment should be more stringent under this section as compared to the earlier section under Information and Technology Act, 2000. Section 67B's proviso provides that this section doesn't extend to any pamphlet, book, paper, drawing, or picture, where it has been defended that it is in the interests of public interests or good, or when the religion is the basis for it. Eg., like in ancient temples, there are certain idols, scriptures, sculptures, texts, paintings, books, drawings, etc., is for the education purposes; because these types of things becomes a matter of concern only when it takes the commercialized nature.

[7] *Supra* note 2.
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*
[11] *Ibid.*
[12] *Ibid.*
[13] *Ibid.*

- SECTION 67C: It provides for the punishment for Preservation & retention of information by intermediaries, i.e., up to 3 years or with fine, or both. This section doesn't limit any restriction on imposing fine.[14]
- SECTION 69: It lays down that where the Govt. or any other officer authorized by Govt. in its behalf; if it is satisfied that it is necessary or expedient for maintaining friendly relations with foreign State, maintaining law & order, investigation of offence, security of nation, sovereignty of a nation, integrity of State, etc., can allow for monitoring, decryption & interception of any information to be generated, stored, or transferred. This section only vests this authority to Govt. or its officials, any private can't do this. Moreover, the reasons are to be given by the Govt. or its officials; and in case of any kind of infringement of other's rights, the case comes up before the Court, the Court will see the reasons for doing so. The subscribers and intermediaries should help the Govt. and its officials in doing this task and any omission to provide such information or having access to such data, i.e., the failure to assist the Govt. or Govt. officials, is liable to be imprisoned for a time period which may extend up to 7 years or with fine or both.[15]
- SECTION 69A: It provides for the blocking the access of any person by the Govt. or their authorized persons, if the above mentioned things as per section 69, are fulfilled. And its failure to follow by any intermediary leads to the imprisonment up to 7 yrs or with fine, or both.[16]
- SECTION 69B: It provides that the State Govt. may for enhancing cyber security, preventing any computer contaminant within the country, or for identification of any party, etc., can ask for monitor or to collect any data. And any person in charge of an resource shall be called or any intermediary will be called and they will help in providing that crucial information or data. However, if that such person is in failure to provide with such an information, shall be liable to be punished for a term of 3 years or with fine, or both.[17]

CONCLUSION: Information & Technology Act, 2000 has been considered as a great initiative for bringing about certain cyber offences and cyber crimes to our knowledge, but it has been failed to point out each and every offence or crime which is related with cyber crime. Information and Technology Act, 2000 has been even amended in 2008, by considering certain points; but due to the rapid increase in technology and communication, the crime rate in cyber space has been increasing day by day without any kind of delay. Cyber crimes are wider in its approach, as we compared it with the Information and Technology Act; because the Act fails to deal with each and every cyber crime. The Information and Technology Act, 2000 is lacking due to its following grey areas:

- Not defining cyber crime or cyber offences: The main terms, i.e., the cyber crime and cyber offences have not been defined under the Act anywhere.
- Jurisdictional issue: The Act is silent on the jurisdiction aspect, which is of utmost importance in legal aspects for deciding the place of filing the case.

[14] *Supra* note 2.
[15] *Ibid.*
[16] *Ibid.*
[17] *Supra* note 2.

- Covering of only broad cyber crimes or contraventions: There were only 10 offences initially under the Information and Technology Act, 2000. However, with the advancement in information and technology and in the era of digitalization, with the increased use of technology and communication methods by the criminals, have made it necessary to have an amendment in the Act for the covering of certain more offences and crimes. Therefore, with the Information and Technology (Amendment) Act, 2008; the 13 more cyber offences have been inserted in the Act.
- No parameter for implementation: The Information and Technology Act, 2000, has not prescribed any particular standard of parameter which is necessary for its proper implementation. In India, where neither the Judges, Government, nor the police is pretty much acquainted with the technology and its procedure, it is totally evident that the question of proper implementation of the provisions of the Act is not permissible at all.

After considering each and every pros and cons of the Act, it is pretty much clear that there is a need of proper Act or Code which deals with each and every cyber crime or offence which has been discovered or yet to be developed. The law needed to be relaxed in amending procedure also, because there has been constantly daily increase in the number of the cyber crimes within the country, due to the digitalization. Moreover, in the era of the globalization, it is the instant need of an hour to be regulated by the adequate laws, especially in cyber areas.[18]

[18] *Supra* note 3.