Impact Factor-7.675 (SJIF) ISSN-2278-9308

B.Aadhar

Peer-Reviewed & Refreed Indexed

Multidisciplinary International Research Journal

October -2021

ISSUE No- (CCCXXIII)323

Chief Editor
Prof. Virag S. Gawande
Director
Aadhar Social
Research & Development
Training Institute Amravati

Editor:
Dr.Dinesh W.Nichit
Principal
Sant Gadge Maharaj
Art's Comm,Sci Collage,
Walgaon.Dist. Amravati.

Executive Editor:
Dr.Sanjay J. Kothari
Head, Deptt. of Economics,
G.S.Tompe Arts Comm,Sci Collage
Chandur Bazar Dist. Amravati

This Journal is indexed in :

- **Scientific Journal Impact Factor (SJIF)**
- **Cosmos Impact Factor (CIF)**
- **International Impact Factor Services (IIFS)**

For Details Visit To : ***www.aadharsocial.com*** Aadhar Publications

41	The Indian Cybercrime and the IT Act, 2000 **Dr. Rajesh B. Deshmukh / Miss Aamprapali Vijaykumar Kasture**	181
42	Trademarks: exploring the Function, Object, role and rational **Mrs. Shilpa Dolarkar**	186
43	Right to Health and food safety: What one eats, Always Matters! **Dr. (Mrs.) Vina Vijay Patil / Mrs. Shweta Shetty**	192
44	स्त्री पुरुष तुलनाकार ताराबाई शिंदे भारतीय स्त्रीवादाच्या जनक प्रा.डॉ.गोविंद म. गायकी	197
45	बालकांना लिंगभाव (स्त्री—पुरुष) समानतेचे शिक्षण – एक अध्ययन प्रा. शैलेश बाबुराव पाटील	199
46	संस्कृत साहित्य कोश : आधुनिक संस्कृत साहित्यातील एक दीपस्तंभ डॉ. भगवान नारायण पंडा	202

B.Aadhar International Peer-Reviewed Indexed Research Journal

Impact Factor -(SJIF) -7.675,Issue NO, 323(CCCXXIII)

ISSN : 2278-9308 October, 2021

The Indian Cybercrime and the IT Act, 2000

Dr. Rajesh B. Deshmukh LL.M. Ph.D.(Law) [1]

Miss Aamprapali Vijaykumar Kasture [2]

Introduction

If one has asked to quote one of the greatest revolution that has put great impact on the civilisation, he will hardly hesitate to point out the information revolution!!! He impact the digital technology has radiated is too intensively modified the present civilisation and the effect deeply transformed the world ever. It boosted up the human potential, break up the boundaries of time and space, change the way we navigate, robots are on the verge of replacing human at critical locations, AI swapping the human ability, to quote a few.

The present age is the age of 'automation' where man is shifting his maximum burden on machines to get work done. The Computer Technology helps the present human civilization to such a greater extend that life without computers seem to be impossible! Speaking with examples, railway reservations, aircraft transportations, bio-matrix attendance in offices, Examination result cards, Traffic signals, Telephonic communications, Banking transactions, all are now carried out with the help of computer machines and every data and information has acquired electronic shape and capable to move through the optic fibres. Today, voice files, song files, photographs, currencies, news items, clips, bio-data's, letters, so on and so forth are capable of being transferred, distributed, circulated and stored in electronic form. Thus present generation is greatly depends upon the computer technology for the easy mechanism and effective operations operated in electric format through computers.[1]

However, the transformation does not merely lead to pleasant results, but also escorted the society to more unpleasant, deadly, more intensified and draconian terrain of 'cyber criminality'. Cyber criminality has emerged as technology assisted criminality that hardly respect the geographical boarder, individual identity, jurisdictional limitation or any other limitations that physical world poses for the crime commission. Thus person seating in pan American countries can remote execute crime in India, or person may used network of any other country for commission of crime. While commission of crime, multiple jurisdictions may involve posing several challenges to prosecution running on old traditional principles, fragmented with national borders. More dangerous feature of cyber crime is the quality of criminal executing these crime are highly qualified, techno-savvy, intellectual and better understand the legal complexity, and if get traced out, have resources to play with the legal technicality.

---

[1] Associate Professor Shri Shivaji Shivaji Law College, Parbhani (Affiliated to SRT University Nanded (Maharashtra). See, https://mspmslcp.in/faculty/) Any productive suggestions, opinion and criticism for improvement in this article are most welcome and may be addressed at, (email). © Authors

[2] Asst. Police Prosecutor Gr-A, and Research Scholar (Law) at SRT Marathwada University, Nanded (Maharashtra) registered for the Ph.D. programme for research topic entitled, "A Study on Cyber crime and it's investigation with special reference to Pune District' © Authors

[1] See, Chowbe, Vijaykumar Shrikrushna, An Introduction to Cyber Crime: General Considerations (February 21, 2011). Available at SSRN: https://ssrn.com/abstract=1766234 or http://dx.doi.org/10.2139/ssrn.1766234 visited on 25.11.2021.

Cybercrime, as simply describe, is computer related crime, committed through and with the help of computers. Cybercrime is misnomers terms or slang, as the word has never been defined anywhere, but instead the statutes employ the phraseology 'offence'[2] to denote any act that is prohibited by law. Even the Information Technology Act, 2000 that enacted to regulate the cyberspace employ the word 'offence'[3] to denote any act or contravention committed in cyberspace.

However, it has need further deliberations that everything that committed in cyberspace cannot be directly jumped to conclude that it is cybercrime. The Information Technology Act, 2000 that proposes to deal with the technology based offences has adopted two different approaches for the offences committed against or with the help of computer technology. Thus, in the first category, where computer technology is merely an instrumental, carrier and used as means to achieve the object cannot be considered as cybercrime in strict sense. In such cases computer is merely a means, an instrument, a choice to commit a crime. Thus offences like fraud, defamation, terrorism, child abuse, extortion, misappropriation, abetment, corruption can be committed with our without computer technology. These offences are already known to the traditional criminality and there is mechanism set for addressing such offences. However, there are offences, which are committed against the computer where computer technology itself is target, such as virus plantation, data theft, hacking, stalking, denial of service attack which only happen against, on, or with the computer technology. There, the Information Technology has adopted following approach-

1. Offences where computer technology has been used merely as an instrument, as means only to commit offences; such offences shall be dealt with the traditional method by applying the known enactments, however, since the computer technology has been involved, and during trial the use of the computer technology is required to be established, the electronic evidence, digital documents shall be authenticated with the help of the provisions of IT Act, 2000.
2. Offences where computer technology itself has been targeted, as an object, and act itself hamper the computer technology shall only be and separately dealt by the IT Act, 2000. Such offences are listed in the Act, and more specifically under Chapter – XI of the act.

Thus, everything that has been happened in cyberspace cannot be dealt by the IT Act, 2000, but only the offences or contraventions committed in cyberspace against the computers, computer networking, any electronic gadgets, such as data theft, denial of service attack, virus plantation, hacking are purely fall in this category.

Therefore, if offence of 'cheating' has been reported by using mobiles, the offence will be booked under IPC, 1860 with relevant section,[4] read with IT Act, 2000 as computer technology has been involved and therefore investigation of offence, evidence collection,

[2] For example, See, S. 40 of the Indian Penal Code, 1860 where the word offence has been defined to any act in contravention of legal provision. S.40. of IPC, 1860 : **"Offence".**—Except in the 2 [Chapters] and sections mentioned in clauses 2 and 3 of this section, the word "offence" denotes a thing made punishable by this Code. (this definition to certain variation also apply to special punitive enactments.

[3] Chapter XI of the Information Technology Act, 2000 specifically dealt with 'Offences'

[4] S. 415 to S. 420 of the IPC, 1860.

forensic formalities, may be done under various provisions of IT Act, 2000. Therefore, in order to understand the Cyber criminality it is essential to glance through the IT Act, 2000. The preamble and objectives of the IT Act, 2000 revealed that the enactment proposes to give legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information an further to facilitate electronic filing of documents with the Government agencies. Act also amended the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers' Books Evidence Act, 1891; and the Reserve Bank of India Act, 1934 to make it amenable and compatible for addressing issues arsing out of and incidental thereto the computer technology.

Apart from the same, initial act of 2000 had also has provisions to deal with few of the computer related offences like 'hacking',[5] virus etc. Chapter XI of the Act has more elaborative and added more offences in the list. The definition related to various contraventions and offences further elaborated to make the IT Act, 2000 relevant and incidental and capable to deal with the more complex incidences, such as defines the terms access in a computer network in section 2(a); computer in section 2(I); computer network in section (2j); data in section 2(0); and information in section 2(v). These are all the necessary ingredients that are useful to technically understand the concept of Cyber Crime. In a cybercrime, the computer or the data are the targets or the object of the offense or a tool in committing some other offense. The definition of the term computer elaborates that computer is not only the computer or laptop on our tables, as per the definition computer means any electronic, magnetic, optical or other high-speed data processing devise of the system which performs logical, arithmetic and memory function by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network. Thus Information Technology and Globalization lead superhighway on the path of development and progress. Now Cyber criminality has now become non-separable part and if global consensus is in favour adaptation of Globalization & Information Technology, Cyber criminality has to be accepted as non-optional phenomenon as an integral part of it. Cyber criminality is now as real as Globalization and Information Technology, and there is hardly any way out. Only way out is to overcome the threat pose by Cyber Criminality, face it without ignoring it![6] Few other prominent features of IT Act, 2000 can be described as -

- In the Information Technology Act 2000 or any law of the country. Cybercrime is no different from traditional crime. The only difference is that cybercrime involves computer technology;

[5] Hacking- If a person 'A' Cyber Criminal sitting in his own house, through his computer hacks the computer of B and steals the data saved in B's computer without physically touching the computer or entering into computer system. However, by the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009) provision of offence of hacking has been removed and the same has been now dealt with the widening scope of S. 65 of the IT Act, 2000.

[6] See for more details, Chowbe, Vijaykumar Shrikrushna, Cyber Criminality & its Legal Control: Fighting with Stones in Jet Age (February 21, 2011). Available at SSRN: https://ssrn.com/abstract=1766235 or http://dx.doi.org/10.2139/ssrn.1766235

- Subject to certain sections of the IT Act, etc., the following points appear prominently;
- Section 77A of the IT Act provides for all offenses under the IT Act, the punishment for which is imprisonment for a period of 3 (three) years or less, subject to certain exceptions;
- The provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 ("Cr.P.C") shall apply in relation to such compound;
- Section 77B of the IT Act provides that notwithstanding nothing contained in the Cr. P. C., all offenses punishable by imprisonment of 3 (three) years and above under the IT Act shall be cognizable and all offenses shall be punishable by 3 (three) years or Imprisonment of less than that shall be punishable be bailable;
- Most cybercrimes covered under the IT Act are punishable by imprisonment of 3 (three) years or less.
- Publishing or transmitting obscene material in electronic form under section 67 of the IT Act;
- Publication or transmission of material containing sexually explicit act, etc. in electronic form under section 67A of the IT Act;
- Publication or transmission of material depicting children in electronic form under Section 67B[7] of the IT Act, clearly stated in the Act, etc.; and -
- Cyber terrorism under Section 66F of the IT Act;
- If a person spreads cyber terrorism or is involved in any conspiracy to do so, he can be sentenced to life imprisonment.

Information technology law defines a few more things, which are as follows: Computer means any electronic, magnetic, optical or any other device that can exchange data at a fast speed, which can be used for different technologies. Able to perform mathematical, logical or

---

7 Section 67B in The Information Technology Act, 2000 runs as under -

[67B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form. -Whoever-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually esplicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either discription for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes.

Explanation. -For the purposes of this section "children" means a person who has not completed the age of 18 years.]

collectible work with the help of. It includes every program and software connected to or related to a computer system.

Conclusion

Thus, it is quite clear that the cyberspace is not only remain the place of amusement, or place to satisfy curiosity, but it is much dangerous place that deal with the privacy, may stalk the women, use the women and children as commodity and hack computers and even attack on information. Therefore it is now required that government must switch over to better security feature to regulate the cyberspace, and even the multinational approach may be adopted to make this place better. The provisions as describe above are useful, but not sufficient to control and regulate the cyber crime. In absence of international cooperation and without helping hands of all stakeholders, the cyberspace will be, and would be become more dangerous place to be live in!!