ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC - NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

Cybercrime Investigation & Evidentiary Aspect Vis-À-Vis Obscenity And Pornography In Cyberspace

Authored By –

Dr. Ashok Wadje[1]

Preface:

Computers, Information Technology, cyberspace and internet world has profoundly changed lives of masses, bringing out extreme transformation in the living style of the people. Thinking of human activities without Information Technology, computer and internet, sounds impracticable. What has changed over the period of time is the life style of human beings in different forms ranging from business environment to education, employment, communication, entertainment, governance, commerce and so on and so forth. Especially this trend is global one, having bearing on the global trends, transaction, trade, business, commerce, international relations and communication. This indeed has replaced many of the classical and traditional usages of communication. Information Technology has blessed the globe with constant and healthy changes terms of what has been mentioned above. Almost everything is online, available on a single click of the user from any corner of the world.

Referring Information Technology, in several of its form i.e. Computer, Computer System, Computer Network, Internet and Mobile or handheld phones and several other electronic and communication devices has brought this change in the society and in the lives of the people. These devices and services of internet in the cyber world is sine qua non for any individual or any entity working in business environment and otherwise. People have actually started interacting very frequently through online devices, bringing them together and more closure like never before. Interaction, communication, exchange of things, goods and services, business activity, governance and inter-state dealings has increased to such a level, that it is unimaginative to revert back to traditional ways of human intercourse of dealing with each other. But if one looks the other side of the coin, this has indeed, exposed us to several problems and complex questions leading to commission of crime or offences codified by the law of the land. No one could have imaged at the time of adopting these technologies that, it

[1] Registrar (I/c) and Associate Professor of Law at Maharashtra National Law University, Aurangabad. The Author is holding Ph.D. Degree in Cyber Law. Email ID of the Author: ashokwadje@gmail.com

ISSN: 2582-6433

might lead us to some unthinkable human activities on cyberspace including commission of several crimes in respect of said technology or with the help of such technology. In this context it is pertinent to mention one quote:

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[2]

"Cyber Crimes": Nature, scope and extent.

Cyber space has today come to denote everything about computers, the Internet, websites, data, emails, networks, software, data storage devices such as hard disks, USB disks etc., and also electronic devices such as cell phones, ATM machines etc. In short, definition of "Cyber law" associates with 'law governing cyber space'.[3] Main concern of this branch is to:

1) Ensure 'Cyber Security and
2) Prevent and curb cybercrimes.

Cybercrimes are, in the era of technocrat world, real threat to the technological driven society, making it difficult to legitimate use of the Information technology and usages. Cybercrimes comes as a threat in many forms and ways in relation to Computer, Internet, websites, data, emails, networks, software, data storage devices etc. Cybercrimes can involve criminal activities that are traditional in nature such as theft, fraud, forgery, defamation and mischief. The misuse of computers has given rise to new age crimes such as hacking, cyber stalking, cyber pornography, web jacking, denial of access, introduction of virus, credit card frauds, financial crimes over or through or with the help of information technology.

Nature of cybercrimes is challenging and requires new definitions and understanding and a restatement of accepted norms of criminal conduct and punishment because of several reasons.

It could be defined in simple words as, "any illegal act that involves a computer, computer system or computer network."[4] Moreover, when it comes to a particular legislation relating to cyber law dealing with the "cybercrime", there is further classification as to 'cyber contraventions' and 'cybercrimes'. The former is lesser sever and doesn't take into consideration mens rea i.e. intention behind the crime and later based on intention to commit offences. In fact it is more about degree and extent of criminal activity rather than anything

[2] NATIONAL RESEARCH COUNCIL: COMPUTER AT RISK, (National Research Council, USA)(1991), National Research Council, USA.
[3] ROHAS NAGPAL, FUNDAMENTALS OF CYBER LAW, 7, (Asian School of Cyber Law) (2009).
[4] VAKUL SHARMA, INFORMATION TECHNOLOGY: LAW & PRACTICE, 160, (Universal Law Publishing Co, 3rd ed. 2011).

ISSN: 2582-6433

else.[5] Functionally, the word 'cybercrime' by its very terminology, restricts itself to the offences committed on the Internet which is a network of computers that communicate each other. It would also encompass offences committed in relation to or with the help of computers. It has also been defined[6] as: "a wide variety of criminal offences and unlawful activities related to or having connection to computers."

As discussed above, with the passage of time and advancement of Information Technology, Cyber world has begun to follow an altogether different path i.e. of taking undue advantages and unlawful gains with the help of IT usages by targeting computer, Information Technology and Cyberspace or with the help thereof, started committing new kinds wrongs to which a new has been coined in all the legal systems of the globe: "Cybercrime". This could be committed with respect to following things[7]:

1) Against person
2) Against property
3) Against Organization/Government
4) Society

Such offences, unlike traditional offences, are unique in terms of its crime causation, *modus operendi*, subject-matter and tools with the help of which it could be committed. Though it was possible to prosecute the culprit of such offences under traditional penal laws[8], it was felt wise by Government to have a separate Act altogether to deal with such type of offences. So Information Technology Act was enacted in the year of 2000, which stipulates number of Cybercrimes, making it an exclusive law dealing with cybercrimes. So now with respect to Cybercrimes, Indian Penal Code is no more applicable when it comes to cyberspace and a case for cybercrime, now, could be registered under Information Technology Act, 2000.

Information Technology Act, 2000/2008 is the source of "Cyber Law" and is widely known as 'Indian Cyber Law,[9]' dealing thoroughly with terms 'cyberspace' and 'information technology'.

[5] *Id*, at 160.
[6] DEVASHISH BHARUKA & AJIT JOY, LEGAL DIMENSIONS OF CYBERSPACE, 228, (S.K. Verma & Raman Mittal eds. 2004, Indian Law Institute).
[7] PRASHANT MALI, CLASSIFICATION OF CYBER CRIME, http://www.lawyersclubindia.com/articles/Classification-Of-CyberCrimes--1484.asp#.UpRyXtKnpoE (last visited on Nov. 26, 2013 at 3:36 pm.)
[8] Indian Penal Code, 1860 and allied laws.
[9] ROHAS NAGPAL, "COMMENTARY ON INFORMATION TECHNOLOGY ACT", at page 9.

ISSN: 2582-6433

Broadly, IT Act, 2000 could be classified under two different parts[10]:

1. For legal recognition of 'e-commerce[11]' and 'e-governance[12]' and
2. For making certain acts as Cybercrimes[13] punishable by Law.

In particular Following is the 'scheme of Offences'[14] as given in IT Act, 2000 and Amended Act of 2008:

1. Tampering with Computer Source Document: Section 65
2. Computer related Offences[15]: Section 66[16]
3. Offensive Messages: Section 66-A
4. Receiving Stolen Computer resource & communication device: Section 66-B
5. Identity Theft: Section 66-C
6. Cheating by Personation by using Computer Resource: Section 66-D
7. Violation of Privacy: Section 66-E
8. Cyber terrorism: Section 66-F
9. Obscenity in electronic form: Section 67 (General obscenity)
    a. Obscenity in electronic form: Section 67-A (Sexual act or conduct therein)
    b. Obscenity in electronic form: Section 67-B (Child pornography)

Before I begin with the theme of the article it is worth to know what is it that Information Technology is all about, its various forms, its functioning as given and contemplated by Information Technology Act, 2000[17] and Information Technology (Amendment) Act, 2008[18] so far as 'cyberspace' is concerned.

"Information Technology" in common parlance connotes anything related to computing technology, such as networking, hardware, software, the Internet, or the people that work with these technologies[19].

[10] DEVASHIS BHARUKA, AJIT JOY, *Computer Crimes*, in LEGAL DIMENSIONS OF CYBERSPACE 232 (S.K. VERMA, RAMAN MITTAL ed., 2004).
[11] Electronic commerce
[12] Electronic Governance
[13] Broadly speaking this has been given under two different heads under IT Act: "Contraventions" and "Offences". Contraventions entail penalty on culprit and offences prescribes and imposes punishment.
[14] Chapter XI of I.T. Act.
[15] In the original I.T. Act, 2000 it was mentioned as 'Hacking with the Computer System'.
[16] To be read with Section 43 of the Act.
[17] Hereinafter referred as "IT Act, 2000"
[18] Hereinafter referred as "Amended I.T. Act of 2008"
[19] Tech Terms.com http://www.techterms.com/definition/it (Last updated on December 29, 2013 at 11:45 am).

ISSN: 2582-6433

"Computer"[20] means *any electronic, magnetic optical or other high speed data processing device or system which performs logical, arithmetic and memory functions 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,"*

Furthermore, with respect to 'Computer' three more terms have been defined under Information Technology Act, 2000 which are to be read with. Those terms are: 'Computer Network'[21], 'Computer System'[22] and 'Computer Resource'[23]

It is pertinent to mention definition of *'Computer System'*, in respect of which original Act of 2000, mentioned certain activities amounting to 'hacking.'[24] But now amended IT Act of 2008 stipulates the said offence with respect or under the head of: *'Computer Related offences.'* [25] Definition of Computer System runs as follows:

"Computer System"[26] means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and cable of being used in conjunction with external files which contain computer programmes, electronic instructions, input and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions."

"Communication Device"[27] *means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image."*

[20] Section 2 (i) of I.T. Act, 2000
[21] Section 2 (j)
[22] Section 2 (l)
[23] Section 2 (k)
[24] Section 66 of old IT Act of 2000: 'Hacking with Computer System':
Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects injuriously by any means, commits hacking.
[25] Section 66 of I.T. Act, 2000: Computer related offences', inserted by Information Technology (Amendment) Act, 2008.
[26] Section 2 (l) of IT Act, 2000/2008
[27] Section 2 (ha)

ISSN: 2582-6433

"Electronic Form"[28] with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device."

Definition of *Electronic form* to be read with two more terms which are defined in the Information Technology Act, 2000, those are: 'Data'[29] and 'Information'[30] in electronic form. Importantly, definition of term "access" is crucial to know about

Cyber Obscenity or Pornography:

The Internet has also come in for its share of criticism over the availability of pornography. The growth of the Internet has created an entirely new medium for the dissemination of any message, images, pictures including pornographic one. Not only content has been criticized, but also its ready availability for users of all ages. The worldwide nature of such material as well as the ability to download images makes the system virtually impossible to censor.

This is about general obscenity. The problem is graver when we talk about cyber obscenity. For that matter we need to see firstly what does mean by obscenity off-line. Off-line obscenity covers generally, language, literature or representation dealing with erotic, pornographic and sexually perverted subjects. But the obscenity of any matter lies in its effect on the mind of the reader or viewer more than in any definable quality of the matter itself.

It is difficult, if not impossible, to define the word "obscene" satisfactorily, whether off-line or on-line and to fix the person by whom and the standard by which the obscenity or otherwise of a matter is to be judged.

Although the word 'obscene' is not defined in the Indian Penal Code (as it simply makes certain acts as an offence), the judiciary have had an occasion to distinguish obscenity from art and literature that contains sex and nudity by stating that it is necessary to decide whether the obscene information is lascivious and may deprave minds who find pleasure in such things. Supreme Court of India, in the case of K. Abbas v. The Union of India & another[31] made a distinction between 'Sex' and 'obscenity' and has observed that, it would be wrong to perceive nudity & sex as essentially obscene, indecent or immoral. 'Sex' & 'obscenity' are not always synonymous."

[28] Section 2 (r)
[29] Section 2(o)
[30] Section 2 (v)
[31] AIR (1970) 2 SCC 780

ISSN: 2582-6433

This approach of Supreme Court has thrown some light on the definition of what amounts to obscene work so far as restriction or regulation thereof is concerned. Obscene word is generally used in relation to a work, if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is. if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it .

Moreover, Information Technology Act, 2000 too has not provided any definition of the term 'obscenity' but provided the same guidelines as is provided by sub-section (2) of Section 292 of Indian Penal Code, 1860. Also it makes certain acts, in relation obscenity in electronic form, as punishable. The only difference is that Information Technology Act, 2000 regulates obscenity on electronic format.

Investigatory & Evidentiary aspects involved in Cyber Obscenity or pornography:

Cyber pornography is one of supreme menace online world is facing, of all the cybercrimes which are being committed on web or internet. It has become a form of business to be carried out on internet and has captured online market.

The said content is available on numerous websites depicting pornography including child pornography. In most of the countries child pornography is banned but pornography per se has not made illegal. As discussed above, cyber pornography includes pornographic websites, pornographic magazines and related information produced using web and computer resources. The said content is available generally for following purposes:

1. Viewing of pornographic or obscene content
2. Downloading the said content
3. Publishing or distributing the said content

This is generally takes place by registering a domain name using fictitious details and host a website on a server located in a country where cyber pornography is not illegal. The suspect accepts online payments and allows paying customers to view/download pornographic or obscene pictures, video etc. from his websites[32].

[32] ROHAS NAGPAL, INTRODUCTION TO CYBERCRIME INVESTIGATION, 4, (2009) Asian School of Cyber Law.

ISSN: 2582-6433

Problem is grave in relation to 'child pornography' which is illegal in most of the countries and that too a mere 'viewing' of child pornography is now an illegal activity. In addition, publishing and transmitting obscene content is hit by Section 67 of IT Act, 2000. Routine filtration of such site is recommended by internet service providers. For blocking child pornography on web, Information Technology (Procedure and Safeguards for blocking for access of information by Public) Rules 2009 and the same is possible either on a complaint before Police or ISP is contacted for blocking such sites or a court order is required.

Cybercrime investigation refers to the collection, analysis and investigation of digital evidence and cyber trails.[33] Generally speaking, digital evidence or electronic evidence is a kind of information stored in or transmitted in digital or electronic form. Digital evidence and cyber trails may be found in computer hard disks, cell phones, CDs, DVDs, floppies, computer networks, the Internet etc. It can be hidden in pictures, encrypted files, password protected files, deleted files, formatted hard disks, deleted emails chat transcripts etc.

Moreover these evidence could also be found in e-EVIDENCE can be found in emails, digital photographs, ATM transaction logs, word processing, documents, instant message histories, fi les saved from accounting programs, spreadsheets, Internet browser histories databases, contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files. Digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available.[34]

Digital evidence can related to several offences as given in the Information Technology Act, 2000 or Information Technology (Amendment) Act, 2008, ranging from or related to Computer related offences or hacking, cyber pornography, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service cyber defamation, cyber terrorism etc.

In particular Cybercrime investigation and evidentiary aspects involved in the Cybercrime is a part of Forensic Science and generally referred as 'Cyber Forensic'.[35] It is pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also

[33] *Id* at 40.
[34] ADV. PRASHANT MALI, ELECTRONIC EVIDENCE & CYBER LAW. https://37c96d72-a-1c2e865b-s-sites.googlegroups.com/a/prashantmali.com/prashantmali/CSICommElectronicEvidenceCyberlaw.pdf?attachauth=ANoY7criL2is4g8HPWIcwS2PAQWL94gLmsQ44_tkxMMKHSInfADWwroDfOXdru9EWZRNLBmPVtTSBQYNwI5paBxoZDRM5lklgFEwSRsnQQxBvyzL_LXPT9gyyqcVqm3wjCxzmuGn6f_ZQvq8Bt4oAwUR7oW5cAD9EgHLGP57RSvS4QbaN75dLTWgeDSEluMr-bl76usVy0fgFpVeYvVVplCi19jaF3E-Yjps982cLwYfZPkk0nfCAcPKM6WwdRPoSBqMTcm&attredirects=0 (Last updated on December 31, 2013 at 1:47 pm).
[35] *Id.*

ISSN: 2582-6433

known as digital forensics. Evidence is not only limited to that found on computer but may also extend to include evidence on digital devices such as telecommunication or electronic multimedia devices.

Because of the complex and complicated nature of cybercrimes and in particular cyber pornography or obscenity, law had to respond towards these crimes specifically, covering this as an altogether a separate branch under the head of "cyber law" mostly dealing with regulation, detection, and prohibition of cybercrimes. As discussed above, Information Technology Act, 2000/2008 is Indian cyber law dealing exclusively computer related aspects including cybercrimes. In this connection, legislature had to amend certain related legislations such as Indian Penal Code, Indian Evidence Act, and Banker's Book Evidence Act. Indian Evidence Act, 1872, has been amended in particular to include aspect of *'digital evidence'*. The definition of 'documentary evidence' has been amended to include all documents, including electronic records produced for inspection by the Court.

Article 9 (2) of the UNICITRAL[36] Model Law provides that any information which is electronically stored shall be given its due evidentiary weight. In assessing its weightage, the Model Law provides that due consideration must be given to reliability of the manner in which data message was generated, stored or communicated, to the reliability of the manner in which integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor. This provides clear guidance to examine the weightage that must be given to electronic evidence.

Let us have a look some of the provisions of Indian Evidence Act which are related to cyber investigatory and evidentiary aspects:

1) Section 3 of Evidence Act, 1872 defines "Evidence" means and includes--

"Evidence" means and includes--

1. *all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;*
2. *all documents including electronic records produced for the inspection of the Court; such documents are called documentary evidence.*

In this context it is pertinent to note that the term 'electronic record[37]' has been given the same meaning as that assigned to it under Information Technology Act. Information

[36] United Nations Commission on International Trade Law
[37] Section 2 (t) of Information Technology Act, 2000.

ISSN: 2582-6433

Technology Act provides for:

> *(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.*

2) Section 17 of Evidence Act, 1872 provides for 'admission'. This definition has been changed to include a statement in oral, documentary, or electronic form which suggests an inference to any fact at issue or relevance.

3) Section 22-A has been inserted into Evidence Act to provide for the relevancy of oral evidence regarding the contents of electronic records. It provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question.

4) Section 65-A and 65-B are introduced to the Evidence Act, under the Second Schedule to the IT Act. Section 65-A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65-B. Section 65-B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic form, is deemed to be a document and is admissible in evidence without further proof of the original's production, provided the condition set out in Section 65-B are satisfied.

In this context, before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required. It is pertinent to refer to few judicial pronouncements with respect to evidentiary aspect of cybercrime prosecution where judges are beginning to recognize and appreciate the importance of digital evidence in legal proceedings.

In the case of **Bodala Murali Krishna V/s. Smt. Bodala Prathima**[38] court held that the amendments carried to the Evidence Act demonstrates that the emphasis, at present, is to recognize the electronic records and digital signatures as admissible pieces of evidence.

Supreme Court in **State of Maharashtra V/s Dr. Praful B. Desai**[39] the question involved was whether a witness can be examined by means of a video conference. Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence. The court allowed the examination of a

[38] (2007 (2) ALD 72)
[39] AIR 2003 SC 2053

ISSN: 2582-6433

witness through video conferencing and concluded that there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence.[40]

But when it comes to the requirement of evidence that too, in the case of digital or electronic evidence, in the context of cyber obscenity or cyber pornography position of law is somewhat difficult. So far as obscenity on *Internet* or in *electronic form* is concerned it is available in different forms, such as:

- Picture
- Short animated movies
- Sound files and
- Stories
- Different communications etc.

Moreover internet also makes it possible to discuss Sex (literature, queries, consultations, chat groups, etc.), see live sex video footage, etc.

Indian Law i.e. **Section 67** of the **Information Technology Act, 2000** and also **amended Act of 2008** prohibits "obscenity on internet or in electronic form." An *analysis* of this section is:

- Acts which:
  - Publishes
  - Transmits
  - Causes to be publishes
- "Any material"
  - Video files, audio files, text files, images, animations and also
  - CDs, Web sites, Computer, Cell Phones etc
- Which is-
  - Lascivious
  - Appeals to prurient interest
  - Tends to deprave or corrupt of minds of the persons.

[40] ADV. PRASHANT MALI, *Supra* note 34.

ISSN: 2582-6433

How to trace an offender:

Investigation of crime on the crime is highly difficult task and all those methods which are there for detection of crime are still in its infancy. Difficulty arises mostly because of techniques which could be employed in concealment of crime in cyberspace. In fact, cyber criminals are much ahead of present investigation mechanism.

Indian Legal system has a long way to go; to establish a perfect mechanism for investigation, detection and preventing cybercrimes. It's not that Information Technology Act, 2000 is futile and incomplete to deal with these offences, what we are lacking is the "effective enforcement mechanism".

In USA, FBI seeks assistance of National Security Agency established for that purpose. These two bodies work in tandem in cases of Cybercrime and investigation thereof.[41]

Nevertheless, on the basis of following things, it would be easy to trace the offender or cybercriminal in case of Cyber obscenity or pornography:

1) Tracing the origin of Computer, computer system, and Computer Resource or Communication device used for the purpose.

2) Computer Logs

2) IP number of offender, route taken by the offender.

3) With the help of Intermediary or Internet service Provider, whichever applicable.

4) With the location of server.

5) Role of Intermediary: Intermediary could be Cyber Cafe owner, Search Engines, ISP's, Telecom Service Providers, Web-hosting service providers, Network service providers etc. etc. In rare cases these may be held liable, or they may be taken as a help in tracing the offender, since under IT Act, a Government is authorized to call upon "intermediaries" to render every such assistance. In most of the cases ISP will not held liable for "third party information".

Most pornographic websites are hosted in countries where cyber pornography is not illegal. In case the website can be traced to India or some other country where pornography is illegal, then the suspects can be traced using the IP address.

So as to facilitate the trial and investigate the litigation or dispute involving cyber obscenity or pornography following mechanism is designed:

1) Cyber Cells are specifically established for the purpose of investigation and detection of

[41] FEDERAL BEARUO OF INFORMATION, http://www.fbi.gov/about-us/cirg/investigations-and-operations-support/investigations-operations-support (Last updated on December 31, 2013 at 10:30 am).

ISSN: 2582-6433

cybercrime (These cells are very active in Mumbai, Chennai and Delhi).

2) Help of Cyber Professionals or Professional cum ethical hackers and

3) As mentioned above, help of ISP's and/or intermediary can be sought. Intermediaries play a vital role in cybercrime investigation.

4) Moreover during trial of a case, Court may order or ask for the help of any Cyber Professional recognized or authorized by the Government of India, whether for Expert opinion or assistance or as an *amicus curiae.*

Well, often Information Technology Act, 2000 was subject matter of criticism for being toothless legislation, but by virtue of amendment by Information Technology (Amendment) Act, 2008[42], a special power is vested on the Central Government or State Government or authorized officer to intercept, monitor or decrypt any information through any computer resource it considers necessary, for investigation of any offence. By virtue of this provision or power any information generated, transmitted, received or stored in any computer resource can be intercepted and any intermediary or subscriber may be called upon to provide the required information failing which such person is liable to be punished.

Moreover, Central Government is empowered to appoint any department or agency of the Central Government or State Government as Examiner of Electronic Evidence by virtue of Section 79A of IT Act to provide expert opinion on electronic evidence before any court or authority. The said 'electronic evidence' as mentioned above includes computer evidence, digital audio, digital video, cell phones, digital fax machine as explained in the Explanation to Section 79A. The appointment of examiner of electronic evidence is a positive step in strengthening enforcement of cyber laws in India.

Fixing liability:

The persons who create and maintain the pornographic websites are liable. In some cases cyber café owners and managers may also be held liable in case they knowingly allow their customers to access the pornographic websites. When it comes to cybercrime in particular Cyber pornography or obscenity, an offender or person who could be held liable is dependent on numerous factors. A person who is liable therefor could be:

1. Originator of impugned content
2. A person who has made available, an online platform for such act.
3. A person who has actually uploaded the information or

[42] Section 69 of Information Technology Act, 2000.

ISSN: 2582-6433

4. A person who has distributed or hosted or circulated the impugned content or
5. An owner of website or
6. An Internet Service Provider or
7. An Intermediary

Before coming into force of Information Technology (Amendment) Act, 2008, an Internet Service Provider[43] was not liable for any third party information or data made available by him if he could prove that the offence or contravention was committed without his knowledge or he has exercised due diligence to prevent the commission of such offence or such contravention and the burden of proof of lack of knowledge or exercise of due diligence was placed on the Intermediary. In this context a reference must be given to the judicial decision in **Avinash Bajaj V/s State**[44] where an intermediary failed to prove lack of knowledge and adoption of due diligence parameter to escape liability under the IT Act, 2000. Court observed that the Director and CEO of Bazee.com could not prove lack of knowledge and that he had adopted due diligence in performing its duties when a third party placed a DPS MMS clip on its auction site Bazee.com. The court not only held that ISP could not escape liability under Section 79 of IT Act, 2000 but also explained a very important aspect of vicarious liability *vis a vis* ISPs.[45]

But now as per Information Technology (Amendment) Act, 2008, the onus is on the aggrieved party and Internet Service Provider (ISP) is not liable for any third party information, data, or communication link made available or hosted by him, if it observes due diligence in performing its duties and complies with guidelines provided by Central Government.

Conclusion:

Of all the cybercrimes that are committed on internet or on web through or with the help of computer, 'cyber obscenity or pornography' is being committed rapidly and frequently. The said content is available on a single click by the user accessing any website on web from any corner of the world. Manner of detection, investigation, proof and prescribing liability in case of cybercrimes in general and cyber pornography in particular is different, difficult, complex and contentious from that of conventional type of investigation & proof of crime.

[43] Covered under the definition of 'Intermediary'
[44] Popularly known as *Bazee.com case*/DPS MMS clip case **(**2005 DRJ 576)
[45] KARNIKA SETH, COMPUTERS, INTERNET AND NEW TECHNOLOGY LAWS, 462 (1st ed., 2012).

ISSN: 2582-6433

Since it is committed through use of technology, the first task here for the Law enforcement agency would be to get well versed with the technology by understanding its dodges and nuts and *bolts*. Training of law enforcement agency or personnel is the need of the hour, so as to keep pace with the investigatory aspects of cybercrime. Secondly, India cyber law needs to be in consonance with the international information technology law so as to have and ensure uniformity of cyber law which ultimately facilitates the cyber investigation including detection thereof, since the very nature of cybercrime is global and universal and could be committed from any corner of the world which can have a global impact.

Moreover, India needs to a Cyber Crime Convention which deals with the transnational organized crimes including cybercrimes. A joint effort is required at national and international level and combined efforts of government, technical industry, law enforcement bodies and the general masses will lead to tangible results.