

Volume 5, S2: 2018 (November)
Impact Factor 6.0176 (ICI)

ISSN:2455-0418 (Print),
2394-9724 (online)

International Journal of Law, Education, Social and Sports Studies

(IJLESS)

A Peer Reviewed (Refereed) International Research Journal
<http://ijless.kypublications.com/>

One Day National Conference on

“Cyberspace and Cyber Laws”

On November 16th 2018.

School of Law
Sathyabama Institute of Science and Technology

(DEEMED TO BE UNIVERSITY)

Chennai-600119

Accredited with “A” grade by NAAC

www.sathyabama.ac.in

Organizing Committee

Chief Patron

FOUNDER CHANCELLOR COL. Dr. JEPPIAAR

Dr. Tmt. REMIBAI JEPPIAAR

Chancellor, Sathyabama Institute of Science and Technology

Patrons

Dr. MARIE JOHNSON, B.E.,M.B.A.,Ph.D

President, Sathyabama Institute of Science and Technology

Dr. MARIAZEENA JOHNSON,B.E.,M.B.A.,Ph.D

Pro-Chancellor, Sathyabama Institute of Science and Technology

Convener

Dr. Dilshad Shaik

Dean, School of Law

Organizing Secretary

Ms.K.Sofia

Assistant Professor, School of Law

Internal Advisory Committee

Dr. S. Sundar Manoharan, M.E.,Ph.D,Vice Chancellor SIST

Dr.A.Wilson Aruni DVM,Ph.D.,FAMPV,FIAAM

Dr. T. Sasipraba, M.E.,Ph.D., Pro vice-chancellor

Dr. S. S. Rau, M.B.A.,Ph.D.,Registrar

Dr. E. Logashanmugam, M.E.,Ph.D,Director Administration

Dr. B. Sheela Rani, M.E.,Ph.D.Director Research

Dr. Igni Sabasti Prabu, M.E.,Ph.D.,Controller of Examinations.

Dr. N. Kannan M.B.A., LL.B., Ph.D,Professor, School of Law

National Advisory Committee

Prof.Dr.Vijender Kumar,

Vice Chancellor ,Maharashtra National Law University, Nagpur

Prof. Dr. A. David Ambrose

Dept. of Legal Studies, University of Madras

Prof. T.V. Subba Rao

NLISU, Bengaluru

Dr.R.Revathi

Associate Professor TNDALU, Taramani ,Chennai

Prof.Dr.T.Sita Kumari

Professor, Department of Law, SPMVV ,Tirupati

Dr. N.Ravi

Associate Professor, Dr.AGLC,Puducherry

Mr.Sanjay Pinto

Advocate, High Court of Madras

Conference Co-Ordinators

Ms. V. Vijayasri, Assistant Professor

Dr. T. Ambika, Assistant Professor

Mr. Mohammed Salihu, Assistant Professor

MESSAGE



Dr. MARIE JOHNSON

B.E., MBA., M.Phil., Ph.D.

President



Dr. MARIA ZEENA JOHNSON

B.E., MBA., M.Phil., Ph.D

Pro Chancellor

The foundation of Sathyabama Institute of Science and Technology is laid on the essence of academic pursuit and excellence. Excellence in any work can be achieved with utmost dedication, hard work, and perseverance. In the endeavour of fulfilling the dreams of **our founder Chancellor and visionary Col.Dr.Jeppiaar** , Sathyabama Institute of Science and Technology is dedicated to its responsibility and added several achievements and accolades to its 30 years of existence and for its excellence in creating a society that is humane, inclusive and beneficial to all. Research and development forms the backbone of our curriculum at Sathyabama Institute of Science and Technology. The staff and students are engaged in various innovative research activities. Every school of our Institute organizes conferences and seminars frequently on contemporary and relevant topics in order to facilitate research in those areas which will lead to necessary metamorphosis in the academia as well.

The School of Law, right from its inception, has been active in research and has setup an ambient academic environment for its students. With the commitment of highly qualified and efficient staff, the school endeavors vigorously to make a mark in the field of research and development. The One day National Conference on Cyber Space and Cyber Laws organized by the School of Law provide a platform for academicians – teachers, students, research scholars, and industry personnel to discuss on contemporary issues in Cyber Space.

We wish the conference all the very best and urge all participants to brainstorm on the various thrust areas of the conference. We also wish all of you a happy stay in our campus and look forward to your participation in various academic events in the campus.

Ms. Sharmu Rajan
Deputy Superintendent of Police (U/T)
Kanchipuram District

MESSAGE

Dr. Dilshad Shaik
Dean, School of Law
Sathyabama Institute of Science and Technology

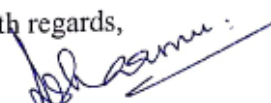
Dear Madam,

I am happy to learn that the School of Law, Sathyabama Institute of Science and Technology is conducting a one day National Conference on "Cyber Space and Cyber Laws" on 16th November 2018. In present times, internet though offers great benefit to the society, also presents opportunities for crime using new and highly sophisticated technology. Due to the massive spread of internet, rapid development of information technology and telecommunications, emails and social networking sites have become the preferred means of communication, in turn cyber crimes are on the rise and it is regarded as a biggest threat to national security leading to the evolution of new forms of transnational crimes more than terrorism. The need of the hour is to achieve perfection in all spheres including law making, enforcement, educating the users in order to protect the personal and sensitive data at the earliest, to avoid the increasing level of victimisation in cyberspace.

In this context, it gets more significant for the School of Law, Sathyabama Institute of Science and Technology to have the opinions of the experts on various aspects of cyberspace with deliberation by participants and to bring out a paper that will certainly be of much help for the betterment of the human kind.

I wish the conference and the School of Law, Sathyabama Institute of Science and Technology a grand success in bringing out an appropriate solution in the form of suggestions to the international community as a token of contribution for the safety and prosperity in the cyberspace.

With regards,



(Sharmu.R)

Editorial Board

Dr M BOSU BABU. PhD
Editor-in-Chief
(Education, Sports and Social
Sciences)
Principal, Sri M.G.Degree College
Acharya Nagarjuna University

Mr.DONIPATI BABJI MA., BL.,
Editor-in-Chief (Law),
Advocate
Guntur, Andhra Pradesh, India
Bar Council of Andhra Pradesh
India

Editorial Team

Dr. Dilshad Shaik,
Dean, School of Law

Ms.K. Sofia
Assistant Professor

Ms. V. Vijayasri
Assistant Professor

Dr. T. Ambika
Assistant Professor

Mr. Mohammed Salihu
Assistant Professor

Ms. V.R.Uma
Assistant Professor, Dr.AGLC, Puducherry

Index

Volume 5, S2: 2018 (November)

S. No.	TITLE	AUTHOR(S)	Page No
1	LEGAL PERSPECTIVE OF UNAUTHORIZED ACCESS IN INDIA-A REVIEW	Dr. Dilshad Shaik, Professor & Dean, School of Law, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu & Ms. V. R. Uma, Assistant Professor in Law, Dr. Ambedkar, Government Law College, Puducherry	01
2	TECHNO-VOYEURISM: A THREAT TO DIGNITY OF WOMEN	Dr. P. Sree Sudha, Associate Professor, Damodaram Sanjivayya National Law University, Visakhapatnam, Andhra Pradesh	10
3	CYBER LAWS IN INDIA: TECHNO-LEGAL CHALLENGES AFFECTING THE ENFORCEMENT	Dr. Nagarathna A., Associate Professor in Law and Co-Ordinator, Advanced Centre for Research Development and Training in Cyber Laws & Cyber Forensics, National Law School of India University, Bengaluru & Ms. Shiyana Sebastian, Research Scholar, National Law School of India University, Bengaluru	24
4	ROLE OF CYBER SPACE IN OPEN AND DISTANCE EDUCATION- AN ANALYSIS	Dr. S. K. Zareena, Assistant Regional Director, IGNOU Regional Centre, Chennai, Tamil Nadu & Dr. A. Pareeth JayaDevi, Assistant Professor, MEASI College of Education, Chennai, Tamil Nadu	39
5	IMPACT OF CYBERBULLYING IN CHILDREN AND YOUTH- A CRITICAL ANALYSIS	Dr. V. Sowbhagya rani, UGC PDF in Law, Sri Venkateswara University, Tirupati. & Prof. V.R.C. Krishnaiah (Rtd), PG Department of Law, Sri Venkateswara University, Tirupati.	45
6	STATUTORY PROVISIONS ON PREVENTION OF CYBER CRIMES- INDIAN PERSPECTIVE	Ms. Sofiya K., Assistant Professor, School of Law, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu.	50
7	VIOLENCE AGAINST WOMEN IN CYBER INFORMATION	Ms. Vijayashri V., Assistant Professor, School of Law, Sathyabama	55

	<i>SUPER HIGHWAY IN INDIA- A LEGAL ANALYSIS</i>	Institute of Science and Technology, Chennai, Tamil Nadu.	
8	<i>REJUNIVATING CYBER LAWS TO SHIELD WOMEN FROM CYBER CRIMES</i>	Dr. T. Ambika <i>Assistant Professor, School of Law, Sathyabama Institute of Science and Technology</i>	63
9	<i>THE SOCIAL IMPACT OF PHISHING ATTACK- AN ANALYSIS</i>	Mr. Mohamed Salihu M., Assistant professor in Sociology, School of Law, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu.	76
10	<i>CYBER MARKET AND CONSUMER PROTECTION IN CYBER SPACE- AN INDIAN SCENARIO</i>	Dr. M. Maya, Assistant Professor, School of Management Studies, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu. & Dr. S. Nithya Assistant Professor, School of Management Studies, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu.	89
11	<i>LEGALITY OF DIGITAL SIGNATURE- A CRITICAL APPRAISAL</i>	Ms. V. Vijaya Lakshmi, Research Assistant, Damodaram Sanjivayya National Law University, Visakhapatnam,	95
12	<i>CONSUMER PROTECTION IN E- COMMERCE: ISSUES AND CHALLENGES IN INDIA</i>	Mr. M.A. Saleem Ahmed, Research Scholar, Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, Tamil Nadu & Prof. Dr. Dilshad Shaik, Research Guide, Vels Institute of Science, Technology and Advanced Studies & Dean, Sathyabama School of Law, Chennai, Tamil Nadu	104
13	<i>CONTRACTING IN CYBER SPACE: CRITICAL ANALYSIS OF LEGAL REGULATIONS OF E- CONTRACTS IN INDIA</i>	Ms. Shanthi Samandha K., Assistant Professor (Law), Andaman Law College, Transport Bhawan, Andaman & Nicobar Islands.	111
14	<i>A CRITIQUE OF CYBER LAW IN INDIA</i>	Dr. E. Ajitha Assistant Professor Department of Bank Management, Ethiraj College for Women (Autonomous)	121
15	<i>JUVENILE CYBERCRIMES AND SMARTPHONE-ADDICTION: A BRIEF REVIEW AND PLAUSIBLE LAW REFORMS</i>	Dr. Kubair Rajiv Gandhi College of Law, Karnataka State Law University & Mr. Dhirendra V., I LL.B. Rajiv Gandhi College of Law, Karnataka State Law University	127

16	<i>EVOLVING CYBER LAW JURISPRUDENCE IN INDIA</i>	P. Prasanna Kumar, Assistant Professor, Sri Kengal Hanumanthaiya Law College.	137
17	<i>CYBER TERRORISM – A THREAT TO WORLD INFORMATION SECURITY AND INTEGRITY: A CRITICAL STUDY</i>	Mr. G. Senthil Kumar, Assistant Professor, School of Law, VISTAS & Mr. Mohamed Zeejin Assistant Professor, School of Law, VISTAS	146
18	<i>CYBER CRIMES ON WOMEN AND CHILDREN- A STUDY</i>	Dr. P. Neeraja, Assistant Professor, Department of Women's Studies, Sri Padmavati Mahila Visvavidyalayam, Tirupati, Andhra Pradesh. & Dr. G. Indira Priyadarsini, Assistant Professor, Department of Law, Sri Padmavati Mahila Visvavidyalayam, Tirupati, Andhra Pradesh.	153
19	<i>CYBER CRIME AND PREVENTIVE MECHANISM- A CRITICAL ANALYSIS</i>	Ms. Ramya Eswaran, Assistant Professor (On Contract), School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Perungudi, Chennai, Tamil Nadu	162
20	<i>PREVENTION OF CYBER CRIMES IN INDIA- AN OVERVIEW</i>	Dr. S. Madhuri Paradesi, Associate Professor, Department of Law, Sri Padmavathi Mahila VisvaVidyalayam, Tirupati, Andhra Pradesh	171
21	<i>PRIVACY AND SECURITY ISSUES IN CLOUD COMPUTING</i>	Mr. Rohit Mishra Associate, Cognizant Technology Solutions	186
22	<i>CRIME AGAINST WOMEN IN CYBER SPACE- AN ANALYSIS</i>	Ms. G. Selvi, Assistant Professor, School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Perungudi, Chennai, Tamil Nadu	192
23	<i>FIGHTING CYBER CRIME: PREVENTION AND PROTECTION</i>	Ms. Bhagavath Harini V. J., I B.A.LL.B. (Hons), School of Law, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu	204
24	<i>THE THREE ORGANS OF CYBERSPACE</i>	Sunidhi Hegde Student, Bangalore Institute of Legal Studies, Karnataka.	211
25	<i>CHILD PORNOGRAPHY IN THE DIGITAL AGE: LEGAL CHALLENGES</i>	Ms. Romita Reang, Research Scholar, Department of Law, North- Eastern Hill University, Shillong, Meghalaya.	222
26	<i>BALANCING OF INTERESTS AND THE CONCEPT OF</i>	Trishna Gurung, Research Scholar, Department of Law, North-	235

	RESPONSIBILITY SHARING VIS-À-VIS CYBER CRIME	Eastern Hill University, Shillong, Meghalaya.	
27	RECOGNIZING PRIVACY AS A FUNDAMENTAL RIGHT - A STEP TOWARDS ROBUST DATA PROTECTION LAW IN INDIA	Ms. Idyath Barakath Nisha N., V B.A.B.L. (Hons), School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Perungudi, Chennai, Tamil Nadu.	245
28	JURISDICTION AND TERRITORIALITY OF THE CYBERSPACE, IN THE ASPECT OF MUNICIPAL AND INTERNATIONAL LAW	Ms. Oviya Nila Muralidharan, IV B.A.LL.B. (Hons), School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Perungudi, Chennai, Tamil Nadu.	254
29	CYBER ATTACKS FROM CRIME TO WAR – PERSPECTIVES IN INTERNATIONAL LAW	Mr. M. Sivaraman, Ph. D. Scholar, School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Perungudi, Chennai, Tamil Nadu & Ms. S. Jeevitha, II B.A.LL.B. (Hons), VIT School of Law, Chennai, Tamil Nadu.	259
30	A STUDY ON CYBER BULLYING WITH SPECIAL REFERENCE TO SCHOOLS AND COLLEGES	Ms. Harshavardhini P., B.B.A.LL.B. (Hons), Saveetha School of Law, Saveetha Institute of Medical and Technical Science, Chennai, Tamil Nadu & Ms. A. Udhaya Sweetline, B.B.A.LL.B. (Hons), Saveetha School of Law, Saveetha Institute of Medical and Technical Science, Chennai, Tamil Nadu	269
31	PSYCHOLOGY AND CHILD PORNOGRAPHY- A COMPARATIVE STUDY	Richu Theresa Robert, III B.A.LL.B., Government Law College, Thiruvananthapuram, Kerala. & Kavya Y.S., III B.A.LL.B., Government Law College, Thiruvananthapuram, Kerala.	276
32	RIGHT OF PRIVACY AND DATA PROTECTION	Prasudha S., IV B.A.LL.B. Integrated 5 Years Course Kerala Law Academy, Law College, Peroorkada, Thiruvananthapuram, Kerala & Chithra B., III B.A.LL.B. Integrated 5 Years Course Kerala Law Academy, Law College, Peroorkada, Thiruvananthapuram, Kerala	287



LEGAL PERSPECTIVE OF UNAUTHORIZED ACCESS IN INDIA-A REVIEW

Dr. Dilshad Shaik,

Professor & Dean, School of Law,

Sathyabama Institute of Science & Technology, Chennai, Tamil Nadu.

&

Ms. V. R. Uma,

Assistant Professor in Law,

Dr. Ambedkar Government Law College, Puducherry

Introduction:

During the last few years the use of computers has grown exponentially. Financial networks, communication systems, power stations, modern automobiles and appliances all depend on computers; and these computers can record withdrawals, deposits, purchases, and telephone calls, usage of electricity, medical treatments, and driving patterns. It is therefore not surprising that computer technology is involved in a growing number of crimes. These are generally taken to include theft of computer services, unauthorized access to protected computers, software piracy alteration and theft of electronically stored information, extortion committed with the assistance of computers, obtaining unauthorized access to records from banks, credit card issuers or customer reporting agencies, traffic in stolen passwords and transmission of destructive viruses or commands. Computer crimes are now a matter of growing concern. Traditional barriers to crime faced by criminals are being obliterated by digital technologies. In a digital world, there are no states or international borders and customs agents do not exist. The information flow effortlessly around the globe, rendering the traditional concept of distance meaningless and the information technology is a *double edge sword*, which can be used for destructive as well as constructive work. Technology is bringing us many new creative possibilities on the one hand, while introducing new and silent dangers on the other.

In the past, the culprit had to be physically present to commit a crime. Now the cyber crimes can be committed from anywhere in the world as bits are transmitted over wires, or by radio waves or over satellite. Similarly, in the past, companies protected their secrets and bank funds in locked file cabinets and vaults in buildings surrounded by electronic fences and armed guards. Now this information is located in one computer service that is connected to thousands of other computers round the world. Anyone of these networks or even a phone line into a company's main computer is a transnational invitation to crime. Crime control requires some system to be in place which ensures that rule violators are identified, apprehended and sanctioned. A criminal using technology can commit thousands of crimes fast and with little



effort. Since much of the conduct involved in committing the crime occurs in an electronic environment, the “physical evidence, if any is evanescent and volatile; and cyber criminals, unlike their real world counterparts can enjoy ideal anonymity. Cyber criminals never have to enter the jurisdiction of the victim-state to commit their crimes. The security is indispensable to E-commerce. Authentication, integrity and confidentiality are the three issues associated with electronic communications. Hacking¹ is a common type of cyber crime committed across the world. Computer hackers may affect the commercial web sites or e-mail system thus paralyzing the electronic business.

HACKING AND CRACKING

Most people would consider a hacker someone who illegally “hacks” into a computer network or system and most likely does something to cause havoc. In the programming community, the person described above would most likely be referred to as a “cracker”. Among programmers and computer people, a hacker is a member of an elite group of extremely talented computer programmers. Cracking is using hacking skills for nefarious or illegal purposes. Cracker is the common term used to describe a malicious hacker. Crackers get into all kinds of mischief, including breaking or “cracking” copy protection on software programs, breaking into system and causing harm, changing data, or stealing. Hackers regard crackers as a less educated group of individuals that cannot truly create their own work, and simply steal other people’s work to cause mischief, or for personal gain. The motivating factors of intruders have shifted from years, but unsurprisingly one thing remains the same the criminal mind takes the path of least resistance. Hacking is so serious that any sensitive data one holds could be lost.

Hacking and cracking are amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into one’s computer systems without one’s knowledge and comments and has trespassed with precious confidential and data information. No computer system in the world is hacking proof. It is unanimously agreed that every system in the world can be hacked. Using one’s own programming abilities, as also various programs with malicious intent to gain unauthorized access to a computer or network are very serious crimes. Hacking² has been defined as deliberately gaining unauthorized access to an information system. Hackers being the delinquent users put computer system out of action, block accesses to information network resources, damage important computer information and programs by using information system and network imperfections and viruses as well. Hacking³ often

¹ A hacker is a person who breaks in or trespasses a computer system. Hackers enjoy exploiting details of programmable system.

² The oxford English dictionary (1998) defines hacker as “a person who or thing that hacks or cuts roughly” or “a person whose uses computers for a hobby especially to gain unauthorized access to data”.

³ Computer hackers may access a computer in order to steal financial information such as credit card access numbers; steal personal information (identity theft); harass (swatting); vandalize; gain access to other



involves more than just unauthorized access to a computer. The cost and inconvenience involved in a hacking incident can be substantial. The handiwork of some hackers as they are known in the computer industry has had disastrous results. No nation is safe from hackers. With the increasing use of computer networks by commercial and military organizations, the potential of hacking was realized by criminals and it became the basis for almost all types of cyber crimes¹.

Hacking related provisions under Indian penal code

Firstly, critically analyze the offence of hacking in terms of Indian Penal Code. The provision, which comes close to describing hacking, is criminal trespass. But to prove criminal trespass under section 441 of the Indian Penal Code, the ingredients of unauthorized entry into or upon property against the will of the person in possession and/or lawfully obtained entry but wrongfully remaining thereon must be satisfied. In applying the section to hacking on the Internet, the prime question that needs to be answered is as to whether website is a property. For this it is imperative to consider the computer or the virtual area of the net as a property. In order to do this we must consider the common jargon used to describe the world of Internet including site, home page, visiting a site and traveling on the super highway are just a few examples. Thus, as trespass actions are grounded in the idea of protecting the owners control over real property, there is no inherent reason as to why the owners control over a websites could not be considered as species of property subject to trespass. It is for this reason that hacking is made a crime specifically punishable under Section 66 (2) of the Information Technology Act, 2000 providing for an imprisonment up to 3 years or with fine up to Rs. 2 lacks or with both.

The next question of importance, which arises for consideration, is when a hacker has no intention to commit any further crimes after having trespassed into the property of other. The question is whether such hacking can be said to constitute intimidation or annoyance. The answer to the question is in the affirmative as any person unauthorized entering into one's property causes annoyance and may result into intimidation. The offence of hacking, if committed with an intention of committing further offences, a parallel for such offences can be drawn from the offences of theft, fraud, mis-appropriation, forgery, nuisance etc. If a person gains unauthorized access to the Property (website/documents) of another, breaching confidentiality of electronic documents, the same is punishable under Indian penal code. Secondly, unauthorized access to commit internet fraud is a form of white-collar crime whose growth is as rapid and diverse as the growth of the Internet itself. In fact, the diversity of areas in which the Internet is being used to defraud people and organization is astonishing.

computers; launch computer attacks; or place malicious software (malware). These are the prevailing crimes committed on the internet.

¹ Bongers W.A. "Criminality and economic conditions" Indiana university press, p.7



Information Technology Act:

India made a modest beginning in responding to cyber crimes by prescribing civil and criminal liabilities for certain activities in cyber space in the Information Technology Act, 2000¹. The borderless cyber-world has created grey areas where existing Information Technology Act, 2000 and Information Technology (amendment) Act, 2008 are open to differing interpretations in the virtual world. It does not deal with crimes in particular. According to section 66 of the Information Technology Act, 2000² “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 it injuriously by any means, commits hacking”. This definition is not only broad but also vague. How one can prove that data has been diminished or affected injuriously if one don't delete or alter any data, just take a peep at it.

The focus of the Information Technology Act was however recognition of electronic records and facilitation of e-commerce. Barely ten sections were incorporated in the Information Technology Act to deal with cyber crimes³. At the time when the Information Technology Act was passed several acts deemed to be illegal in most jurisdictions including virus attacks, data theft, illegal access to data/ accessing and removal of data without the consent of the owner, etc., were listed as civil penalties under the Information Technology Act⁴, 2000.

Offence of hacking only if with dishonest or fraudulent intention

Now, the hacking⁵ of computer is covered under section 66 Information Technology Act only if it is done dishonestly or fraudulently as defined under the Indian Penal Code. If it is not done dishonestly or fraudulently, it would be covered under Section 43 which is civil in nature. Thus, the moment one commits hacking, he would be either criminally liable or face civil liability.

¹ The Information Technology Act, 2000 has been enacted in pursuance to the General Assembly of United Nations resolution n A/RES/51/162, dated the 30th January 1997.

² **India is the 12th nation** in the world that has cyber legislation apart from countries like the US, Singapore, France, Malaysia and Japan.

³ The phrase “cyber crime” is not defined in any enactment in India. This to some extent leads to some confusion whilst enforcing the various provisions spread over the special and general laws, as more fully set out in the Article;

⁴ Section 43 of the IT Act;

⁵ Hacker is a term used to the programming community mean ‘a clever programmer’ and by others, it means ‘some one who tries to break into computer systems’ programmers who use their skills to cause trouble, crash machines, release computer viruses, steal credit card numbers, make free long distance calls (the phone system is so much like a computer system that it is a common target for computer criminals), remove copy protection, and distribute pirated software. This is leading to more confusion. Hackers in the original sense of the term, however, look down on these sorts of activities. Hackers generally deplore cracking.



The Information Technology Amendment Act, 2008 requires the use of “reasonable security practices and procedures,” which it defines as practices and procedures designed to protect sensitive personal information from unauthorized access, damage, use, modification, disclosure or impairment. What constitutes “reasonable security practices and procedures” may be specified in an agreement between the parties or in an applicable law. In the absence of an agreement or law, reasonable security practices may be prescribed by the Central Government. Although this provides little clarity in describing the practices and procedures required, it stresses the need for companies to take a comprehensive and systematic approach to data protection (at least with respect to sensitive personal data).

Section 66 of the Information Technology Act, 2000 under the heading “Hacking” which was misleading was criticized for its ambiguity and for the possibility of abuse. Section 66 of Information Technology Act 2000 defines ‘Hacking with Computer System’¹

Prior to its amendment, the Information Technology Act, 2000 focused more on individual hackers than on systematic data protection. The pre-amendment IT Act imposed liability on any “person” who (among other things) accesses or extracts data from a computer or network without the owner’s permission, damages the data or programs stored on a computer, or denies authorized access to a computer. There is also difficulty felt in interpretation of certain terms under the definition. for instance section 66 of The Information Technology Act, 2000 used the words ‘destroys’ or ‘deletes’ or ‘alters’ ant information and in the case if some hackers intrudes into the systems for ‘fun’ their intention is not to commit any crime. In this instance they just gain access to the system and nothing else.

The language of the Section 66 has now been substituted by new language. Information Technology Amendment Act, 2008 has redefined the term “hacking” as understood by the industry and given it a legal meaning of its own. [Equivalent to cracking] The amendment also takes a broader view of the IT landscape in India by recognizing that corporations and other intermediaries also bear some responsibility in ensuring data in their possession is secure. Failure to do so create a private right of action in the individuals whose sensitive personal information is compromised.

Perhaps one of the more important consequences of the Information Technology Amendment Act, 2008 is that it introduces the concept of personal data into Indian law. The original IT Act punished unauthorized extraction of or damage to data, but it did not explicitly target personal data. The Information Technology Amendment Act, 2008 however, requires

¹ “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 it injuriously by any means, commits hacking. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.”



companies to maintain the security of “sensitive personal data,” thus recognizing that certain data deserves a higher level of protection.

Merger of Section 66 with Section 43

Where human-centric terminology is used for crimes relying on natural language skills and innate gullibility, definitions have to be modified to ensure that fraudulent behavior remains liable no matter how it is committed. One of such attempt is the merging of section 66 and section 43 of Information Technology Act. The simplification measure has been to merge the offences under Section 66 with contraventions under Section 43. Accordingly, a set of deviations have been listed in Section 43 and these have been made subject to civil remedies under Section 43 and criminal prosecution under Section 66.

The intent of the legislature in enacting this section is to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

Protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within the state that lawfully utilize those computers, computer systems, and data. The commonly known crime called hacking has now been entrenched in our law under section 66 of the Information Technology Act which makes any unlawful access and interception of data a criminal offence. This also applies to unauthorized interference with data as contained in section 43.

Now section 66 has to be under stood as follows

- a) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is in charge of a computer resource
 - i. Accesses or secures access to such computer resource;
 - ii. Downloads, copies or extracts any data, computer data base or information from such computer resource including information or data held or stored in any removable storage medium;
 - iii. Denies or causes the denial of access to any person authorized to access any computer resource; he shall be punishable with imprisonment up to one year or a fine which may extend up to two lacs or with both;
- b) If any person, dishonestly or fraudulently, without permission of the owner or of any other person who is in charge of a computer resource introduces or causes to be introduced any computer contaminant or computer virus into any computer resource;



- a. Disrupts or causes disruption or impairment of electronic resource;
- b. Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer resource;
- c. Provides any assistance to any person to facilitate access to a computer resource in contravention of the provisions of this Act, rules or regulations made there under;
- d. Damages or causes to be damaged any computer resource, data, computer database, or other programmes residing in such computer resource; he shall be punishable with imprisonment up to two years or a fine which may extend up to five lacs or with both;

If anyone secures access to any computer without the permission of the owner shall be liable to pay damages of one crore rupees under Information Technology Act.

The saving grace of the Information Technology Act were the amendments carried out to the IPC and Evidence Act, which to some extent provided for prosecution of rampant offences like the Nigerian Scams¹, phishing and other Banking frauds. According to the principle of legality, a criminal law provision may not be given a more extensive area of application than its wording permits. Legal measures to prevent and deter criminal behavior must be clear, at the same time as the introduction of Information Technology in almost every sector of daily life calls for a minimalist approach in order to avoid two different sets of rules and regulations depending on whether a transaction is supported by Information Technology or executed in the traditional environment. Since one of the main functions of the criminal law is to determine which human conducts are regarded as crimes, and given that the advance of society might bring new harmful conducts, the list of conducts prohibited and punished by the legislator through the criminal law is neither fixed nor unchanged forever. The first schedule of the Information Technology Act, 2000 has made certain amendments to the Indian Penal Code.

The definition of electronic records contained in s.2 (1) (t) in the Information Technology Act has also been added as a definition under the Indian Penal Code. All the provisions of the Indian Penal Code, relating to "documents" have been substituted with the term "document or electronic record". The result is that anyone using forged electronic record or certificates is punishable under the IPC for offences related to false evidences and certificates. A number of amendments have been made to sections 29, 167, 172, 192, 463, 464 and the like. The key amendment relates to the widening of term document to include electronic records. Section 464 now recognizes the concept of digital signature.

¹ Such scams are more rampant since 2007, where emails claiming to give out winnings in lotteries; winnings for selected email ids etc., and asking for deposits and payments for customs clearance etc.,



Indian Evidence Act:

The Indian Evidence Act, prior to its being amended by the Information Technology Act, 2000, mainly dealt with evidence, which was in oral or documentary form. Nothing was there to point out about the admissibility, nature and evidentiary value of a conversation or statement recorded in an electromagnetic device. The provisions of modern statutes provide electronic data with the same status as documented evidence. Section 4 of the Information Technology Act, 2000, provides for the legal recognition of electronic records. Similarly section 65A and 65B of The Indian Evidence Act 1872 provides for special provisions as to evidence relating to electronic record and admissibility of electronic records respectively and includes recognition of digital signatures as electronic evidence.

CONCLUSION:

The broad reach of the internet, which connects millions of people worldwide, presents a number of unique challenges to law enforcement to fight against hacking. Technologically sophisticated criminals can exploit the internet's speed and distributed nature to commit hacking and wreak havoc without regard to geographic and jurisdictional boundaries. A single preparatory is able to anonymously take advantage of millions of vulnerable computer neophytes with relative ease. Law enforcement's dilemma is further complicated by the rate at which technological innovations evolve.

Hacking is a new unconventional crime, the emerging legal landscape in relation to cyberspace is not very easy to see and thus to understand the changes. Law codes throughout the world have proved ineffective in curbing the expanding domain of hacking behavior and have a need to re-look and assess the sufficiency of enactment of laws. Law enforcement is bound by physical national boundaries, while hackers are working as combine forces swiftly across borders. Global economic recession has opened another door for cyber attackers to continue their illegal activities and cause potential damage to the world at large making scenario worst. Hacking remains much of activities black box for both lawmakers and those vulnerable to cyber attacks.

It is necessary to "look beyond the surface of law" to recognize "so much that is hidden from view". Deterring and punishing hackers requires a legal structure that will support detection and prosecution of offenders yet the laws defining computer offences, and the legal tools needed to investigate criminals using the Internet, often lag behind social and technological changes, creating legal challenges to law enforcement agencies. But the problem with investigating international cyber crimes and capturing criminals on the Internet is not necessarily due to lack of cooperation among international law enforcement bodies. The issue has much more to do with the fact that the legal systems throughout the world vary greatly and take a very long time to change. These two facts make it extremely difficult for law enforcement



to cooperate, investigate, capture, and ultimately prosecute the cyber criminals who access unauthorized today.

REFERENCES:

- 1) Andrew murray information technology law:the law and society oxford university press (13 may 2010).
- 2) Andrew murray the regulation of cyberspace published november 29th 2006 by routledge-cavendish.
- 3) carlisle george, introduction to information technology law (6th ed) emerald group publishing limited.
- 4) Catherine laberta “ computers are your future :introductory (iith edition) prentice hall publishers (2010)
- 5) Charliglf george “ introduction to information technology communication and ethics in society, vo1.6 iss :3, pp-279-280
- 6) Chonsoria, divya & srivastava, rajeshwar ashok information technology act 2000: a conceptual paradigm shift in law 2006.
- 7) Damaine tembiovi and danilo leoner di and chris mardsden “codifying aberrance-communications self regulation in the age of internet convergence – (2007) rutledge publishers
- 8) Daniel j.solove “the digital person : technology and privacy in the information age (2006) network university press
- 9) Diane rowland and elizereth macdonald “information technology law” cavendish publishing
- 10) George w. Reynolds “ethics in information technology “(2nd edition) july 2006, course publishers.
- 11) I an j. Lloyd “ information technology law – 5th edition – oxford university press, (2008)
- 12) Lloyd, ian j. Information technology law oxford university press, united kingdom, 2007. Paperback. Book condition: new 6th revised edition.
- 13) Michel e. Whiteman and herbert. J mattord “ principles of information security “(2nd edition) course publishers 2004 december
- 14) Stephen haag, and maeve cummings “management information systems for the information age “best book buys publishers (2007)
- 15) The Information Technology Act,2000.



TECHNO-VOYEURISM: A THREAT TO DIGNITY OF WOMEN

Dr. P. Sree Sudha, LL.D. ,

Associate Professor,

Damodaram Sanjivayya National Law University, Visakhapatnam, Andhra Pradesh.

Introduction

The growth of the information society is accompanied by new and serious threats. When internet was invented, inventors did not think for its bad behaviour. However, the criminal mentality of human psychology started its misuse by using internet as a tool of crime, which gave the birth to “cyber-crime” and world is facing a huge challenge from these cyber criminals.¹ People are very reliant on information systems and the internet making them easy targets for cyber criminals.² The number of internet users has grown exponentially over the last twenty years. Cyber-crimes have become rampant in the city.³ Cyber-crime is a major issue facing society today. With the advent of technology, cyber-crime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole.⁴ The cyber-crime is the crime, which occurs in the cyber space. In cyber-crime computer is used as a tool, a target, as incidental, and as associate. Cyber-crime also known as computer crime can be defined as criminal activity directly related to the illegal use of computer and a network, for unauthorized access or theft of stored or on-line data that can be used for several criminal activities against a victim.⁵ Voyeurism is also a cyber crime which punishes a person secretly watches and observes another person or their intimate areas, with lewd and lascivious intent, when that person is in their dwelling, structure, or another location that affords a reasonable expectation of privacy. The crime of voyeurism is considered a misdemeanour. This paper is organized like this. First part of the paper deals with category of cyber crimes committed

¹ Harvey, D “Cyber stalking and Internet Harassment: What the Law can Do” available on: http://www.netsafe.org.nz/Doc_Library/netsafepapers_davidharvey_cyb_erstalking.pdf, visited on 12-3-2018

² Halder, D & Jaishankar, K “The problem of cyber bullying amongst school students in India: The loopholes in IT Act” available on <http://www.careerlauncher.com/1stcontent/plansuppliments/attachment/s/40/64/Cyber%20bullying%20amongst%20school%20students%20in%20India.pdf>, visited on 12-3-2018

³ Halder, D & Jaishankar, K (2008) “Cyber Crimes against Women in India: Problems, Perspectives and Solutions” TMC Academic Journal Volume 3, Issue 1, June 2008 available on http://www.tmc.edu.sg/pdf_files/acadjournal/TMC%20Academic%20Journal%20-%20June%2008%20-%20full%20issue.pdf, visited on 12-3-2018

⁴ Agarwal, R “Cyber Crime Against Women and Regulations in India” available on <http://tmu.ac.in/gallery/viewpointscip2013/pdf/track4/T-403.pdf>, visited on 12-3-2018

⁵ Mirani, S., Pannu, P. & Malhotra, C.(2014). Empowering Women through ICT's: Cyber Campaigns on Violence Against Women in India. Indian Journal of Public Administration, IX (3), 679-695



against women, part two will throw some light on how voyeurism breaches the privacy of women, part three deals with international legal regimes on voyeurism, fourth part will analyze the Indian legal regime on voyeurism it also highlights effective mechanisms for combating voyeurism and finally ends with conclusion.

Cyber crimes are broadly divided into following categories:

- Cyber-crimes committed against persons include various crimes like transmission of obscene messages, harassment of any one with the use of a computer such as e-mail, cyber-bullying and cyber-stalking.¹
- Cyber-crimes against organization or all forms of property. These crimes include illegal and unauthorized computer trespassing, and transmission of important and critical information outside the organization which can lead to a great loss to the organization.
- Cyber-crimes against Government which includes cyber terrorism.

Among the three categories the cyber crimes against women are in increase as per NCRB report. Following section will focuses on cyber crimes committed against women in detail.

1. Cyber Crimes committed against Women

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances. However, the means that enable the free flow of information and ideas over long distances also give rise to a worryingly high incidence of irresponsible behaviour. The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately women are still defenceless in cyber space.² Cyber- crime against women is on at alarming stage and it may pose as a major threat to the security of a person as a whole.³ The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. The widespread circulation of such content is particularly harmful for women. In recent years, there have been numerous reports of women receiving unsolicited emails which often contain obscene and obnoxious language. India is considered as one of the very few countries to enact Information Technology Act (IT Act) 2000 to combat cyber-crimes.⁴ This Act widely covers the commercial and economic crimes unfortunately certain

¹ Duggal, P "Cybercrime" available on <http://cyberlaws.net/cyberindia/cybercrime.html>, visited on 12-3-2018

² Halder, D & Jaishankar, K (2008) "Cyber Crimes against Women in India: Problems, Perspectives and Solutions" TMC Academic Journal Volume 3, Issue 1, June 2008 available on http://www.tmc.edu.sg/pdf_files/acadjournal/TMC%20Academic%20Jo urnal%20-%20June%2008%20-%20full%20issue.pdf, visited on 12-3-2018

³ Jeet, S (2012) "Cyber crimes against women in India: Information Technology Act, 2000" Elixir International Journal Elixir Criminal Law 47 (2012) 8891-8895 available on [http://www.elixirpublishers.com/articles/1351168842_47%20\(2012\)%20 8891-8895.pdf](http://www.elixirpublishers.com/articles/1351168842_47%20(2012)%20 8891-8895.pdf), visited on 12-3-2018

⁴ Sarup, K.(2015). Violence Against Women and Role of Media. Retrieved from: www.scoop.co.nz/stories/WOO501/S00113.htm , visited on 12-3-2018



recent issues like voyeurism still remain untouched in this Act. Social Networking and other websites are created and updated for many useful purposes, but they are nowadays also be used to circulate offensive contents also. Individuals who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of 'cyber- crime'.¹ Women and minors who post their contact details become especially vulnerable. Amongst the various cyber-crimes committed against individuals and society at large, crimes that are specifically targeting women are as cyber-stalking, harassment via e-mails, cyber bullying, morphing, e-mail spoofing, cyber defamation and voyeurism.

1.1 Cyber Stalking

Cyber Stalking is one of the most widespread net crimes in the modern world. The word "stalking" means "pursuing stealthily." Cyber stalking can be used interchangeably with online harassment and online abuse. It is the use of the Internet or other electronic means to stalk or harass a person.² The utilization of technology allows stalkers to harass their target from oceans away. It involves invading the privacy by following a person's movements across the Internet by posting messages on the bulletin boards, entering the chat-rooms frequented by the victim, constantly bombarding the victim with messages and emails with obscene language. While Cyber Stalking affects both men and women, women are disproportionately targets, especially of age group of 16-35, who are stalked by men. It is believed that Over 75% of the victims are female. More than one million women and 370,000 men are stalked annually in the United States. An astonishing one in twelve women and one in forty-five men will be stalked in their lifetimes.³ In Cyber Stalking, stalker access the victim's personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim.

1.1.1 Ritu Kohli Case

The perfectly normal married life of Ritu Kohli, New Delhi turned upside down, when she started receiving a number of emails from an unknown source. Initially she ignored the mails. Stalkers used obscene and obnoxious language and post her residence telephone number and other personal details on various websites, inviting people to chat with her on the phone. As a result, she started receiving numerous obscene calls at odd hours from everywhere, and then she got alarmed. Distraught, Kohli lodged a police complaint. Fortunately Delhi police immediately sprang into action. They traced down the IP address (Internet Protocol address) of the hacker to a cyber cafe. The cyber stalker- Manish Kathuria, later got arrested by the Delhi

¹ Prof. R.K.Chaubey (2012), "An Introduction to Cyber Crime and Cyber law", *Kamal Law House*

² Chakrabart, K.(2013). Gender Justice and Social Media Networking in India: New Frontiers in Connectedness. The Asian Conference on Media and Mass Communication: Official Conference Proceedings

³ Moore, A(2009) "Cyber-stalking and Women - Facts and Statistics" available on <http://womensissues.about.com/od/violenceagainstwomen/a/Cyberstalki ngFS.htm>, visited on 13-3-2018



police and was booked under sec 509 of the IPC (Indian Penal Code) for outraging the modesty of a woman and also under the IT Act (Information Technology Act) of 2000. The case highlighted here is the first case of cyber stalking to be reported in India.

1.1.2 Another Case

In another case of Cyber Stalking that comes in the notice, a 28 year old woman, Neha Ghai was shocked after she received objectionable calls and text messages on her mobile phones and even vulgar e-mails in her inbox. When she approached the cyber cell and lodged a complaint against the accused, she came to know that she has become a victim of cyber stalking and the stalker had collected all her personal details posted on objectionable portals. Cyber stalking nowadays become a serious issue and victims should immediately inform the police. The Police can trace the accused by tracking the IP (internet protocol) address of the system that is used for the criminal activity.

1.2 Harassment Via Email

There is no doubt that email has become one of the most heavily used electronic tools of the last decade. Many people, send and receive in around 100 emails every. Harassment on the Internet can take place in a number of ways. One form may include Harassment through e-mails includes blackmailing, threatening, bullying, constant sending of love letters in anonymous names or regular sending of embarrassing mails to one's mail box. Indian Penal Code, Criminal Procedure Code and select sections of IT Act deal with the protection from cyber-crime. In general they are used to book the perpetrators along with the IPC¹ for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail, according to IPC² for uttering any word or making any gesture intended to insult the modesty of a woman.

1.3 Cyber Bullying

Today, people all over the world have the capability to communicate with each other with just a click of a button and technology opens up new risks. Cyber bullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. Cyber bullying is "wilful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature." Globally, India is third behind China and Singapore in cyber bullying or called online bullying. Cases of suicides linked to cyber bullying have grown over the past decade. Bullying classmates, juniors or even seniors in the school is a common culture among the young school students in India. Social networking sites used in nearly half of cases. Girls are about twice as likely as boys to be victims. With 24 female cases were reported compared with 17 males, reveals that the victims are more often female. India is third on the list

¹ Section 292 A of Indian Penal Code 1860

² Section 509 of Indian Penal Code 1860



behind China and Singapore in the cases of cyber-crime according to a report, highlighting the need to take actions and increase education about online behaviour.

1.4 Cyber Bullying New-Age Threat

Harini (name changed), a 12 year old girl when put up her profile picture on a social networking site, she did not know that she would soon face serious physical threat. When she finally told her parents about the happening, they were shocked that a person living in the neighbourhood had been bullying her and threatening to misuse her personal information and photos if she told anyone. After certain visits to the cyber-crime police station, they somehow managed to get rid of the threat. However, Harini's parents are still not sure how to make their daughter overcome the fear and regain her self-esteem.¹

1.5 Morphing

Morphing is editing the original picture by an unauthorized user. When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads them after editing is known as morphing. It was observed that female's pictures are downloaded from websites by fake users and again re- posted/uploaded on different websites by creating fake profiles after editing them.² This amounts to violation of I.T. Act, 2000 and the violator can also be booked under IPC also for criminal trespass³ committing public nuisance,⁴ for printing or publishing grossly indecent or scurrilous matter⁵ or matter intended to blackmail and for defamation.⁶

1.6 E-mail Spoofing

A spoofed e-mail may be said to be one, which misrepresents its origin [Legal India]. It shows its origin to be different from its actual source. E-mail spoofing is a popular way of scamming online E-mail spoofing is a term used to describe fraudulent email activity in which the sender's address and other parts of the email header are altered to appear as though the email originated from a known or authorized source. By changing certain properties of the email, such as its header, from, return-path and reply- to fields etc., hostile users can make the email appear to be from someone other than the actual sender. Email spoofing is possible because the main

¹ Basu, S. (2013) "Stalking the Stranger in Web2.0: A Contemporary Regulatory Analysis," *EJLT*, 2. Available at: www.ejlt.org/article/viewArticle/142/236, accessed on 12-3-2018

² Cyber Violence against Women and Girls: A World-wide Wake-up Call a Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender (2015). Available at: www.unwomen.org/~media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259, accessed on 12-3-2018

³ Section 441 of Indian Penal Code 1860

⁴ Section 290 of Indian Penal Code 1860

⁵ Section 292A of Indian Penal Code 1860

⁶ Section 501 of Indian Penal Code 1860



protocol used in sending e-mail i.e. Simple Mail Transfer Protocol (SMTP), does not allow an authentication mechanism. Email spoof can cause monetary damage also.

1.7 Cyber Defamation

Cyber tort including libel and defamation is another common crime against women in the net. Although this can happen to both genders, but women are more vulnerable. This occurs when defamation takes place with the help of computers and/or the Internet when someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person. Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. You build a great brand over 20 years and all it takes is 2 days to destroy it, on the Net.¹ Unfortunately cyber defamation is not defined by the IT Act 2000 and it is treated by the criminal justice system under the same provisions of publication of obscene materials in the internet. With the exponential increase in the use of the internet as a medium of communication and sharing of information, chances of use of the web for publication of defamatory content has increased multi-fold and there is a coherent need for a clear law in this area.

1.7.1 Cyber Defamation Case

Abhishek, a teenaged student was arrested by the police in India following a girl's complaint about tarnishing her image in the social networking. Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted on the profile.

1.7.2 Laws against Cyber Defamation

In India According to IT Act 2000,² any person who sends, by means of a computer resource or any communication device any offensive information, shall be punishable with imprisonment for a term which may extend to three years and with fine. The offence of cyber defamation is well explained³ in the IPC by mentioning punishment with simple imprisonment that can be extended up to two years or with fine or with both.

2. Voyeurism

In Digital world, voyeurs use hidden cameras, binoculars, telescopes, zoom lenses, cell phones, and other enhanced surveillance devices to do the same. Sometimes, they record their observations digitally and share such recordings with others over the Internet. There are two ways to define voyeurism as behaviour and as a sexual disorder. As per National Crime Records Bureau (MH), there were 838 cases were registered of Voyeurism. There were 6266 cases of stalking, registered under Section 354B of I.P.C.

¹ *Ibid.*,

² Section 67 of Information Technology Act 2000

³ Section 500 of Indian Penal Code 1872



Oxford Dictionary defines a voyeur is “a person who derives sexual gratification from the covert observation of others as they undress or engage in sexual activities.” In this context, the behaviour is concerned with three things: the surreptitious nature of the observations; the private and intimate nature of what is observed; and sexual gratification. Voyeuristic behaviour may extend not only to the making of the voyeuristic images, but may include distribution of voyeuristic visual representations to others.

A second way to consider voyeurism is as symptomatic of a *sexual disorder*. A sub-group of the persons who engage in voyeuristic behaviour suffers from this sexual disorder. According to the American Psychiatric Association's Diagnostic and Statistical Manual of Mental Disorders defines ‘Voyeurism is viewing some form of nudity or sexual activity, accompanied by sexual arousal. To be classified as a sexual disorder, or a paraphilia, voyeurism must be characterized by observing unsuspecting individuals, usually strangers, who are naked or engaging in sexual activity, for the purpose of seeking sexual excitement.’¹

The voyeur usually does not seek any contact with the victim. The perpetrator may masturbate during the act of voyeurism or, more commonly, afterwards in response to the memory of what he or she observed.² The diagnostic criteria for voyeurism are:

- recurrent, intense sexually arousing fantasies, sexual urges or behaviours involving voyeuristic activity, and
- the fantasies, sexual urges, or behaviours cause clinically significant distress or impairment in social, occupational, or other important areas of functioning.

Many individuals include voyeuristic fantasy or behaviour in a repertoire of sexual fantasies. It is only when these fantasies become a focus for an extended period of time (six months or more) and cause distress or impairment in one's life that this would be diagnosable as a paraphilia. Most voyeurs engage in at least one other sexually deviant behaviour, usually exhibitionism or non-consensual sexual touching or rubbing. There is also evidence that voyeurism occurs at an early stage along a continuum of sexual disorders that may become progressively more coercive and invasive. Approximately 20% of voyeurs have committed sexual assault or rape.

3. Voyeurism – International Response

Voyeurism is a criminal offence in many jurisdictions across the world such as Australia, the United States, Canada, and the UK, which criminalise the capturing of either certain images, or observation of individuals, or both.

¹Meg S. Kaplan and Richard B. Krueger, "Voyeurism: Psychopathology and Theory" in *Sexual Deviance: Theory, Assessment and Treatment* (New York: The Guilford Press, 1997), pp. 297-310, at p. 297.

²R. Karl Hanson and Andrew J.R. Harris, "Voyeurism: Assessment and Treatment" in *Sexual Deviance: Theory, Assessment and Treatment* (New York: The Guilford Press, 1997), pp. 311- 331, at p. 315.



3.1 The Beijing Platform for Action (BPfA) - 1995

In 1995 the Beijing Platform for Action (BPfA) called explicitly on governments to 'take effective measures or institute such measures (emphasis mine), including appropriate legislation against pornography and the project of violence against women and children in the media' (UN, 1995, p.102). The BPfA called on both the media and advertising industries to:

- Establish, consistent with freedom of expression, professional guidelines and codes of conduct that address violent, degrading or pornographic materials concerning women in the media, including advertising
- Disseminate information aimed at eliminating spousal and child abuse and all forms of violence against women, including domestic violence.

At the national level, laws regarding violence against women and girls in countries such as Mexico, Brazil, Argentina, Spain and India list specific actions related to media industries. However, while the BPfA listed the actions, which would achieve gender equality and stop gender-based violence, there is no single formal policy on gender and communication in most countries in the world.

3.2 U.S.A Legal Regime of Voyeurism

The criminal voyeurism statute of some states cover "a place where [one] would have a reasonable expectation of privacy", meaning:

- (i) A place where a reasonable person would believe that he or she could disrobe in privacy, without being concerned that his or her undressing was being photographed or filmed by another; or
- (ii) A place where one may reasonably expect to be safe from casual or hostile intrusion or surveillance.

Given the similarity to voyeurism, a jury might find that placing a hidden camera in a certain location may amount to the torts of outrage or negligent infliction of emotional distress. In New York, a law prohibiting unlawful surveillance has addressed video voyeurism. A person is guilty of unlawful surveillance in the second-degree offense, a class E felony punishable by a term of up to 1 - to 4 years in State prison, if he or she:

- (i) for no legitimate purpose, uses or installs an imaging device to surreptitiously view or record another person in a bedroom, bathroom, changing room, or other specified room; or
- (ii) for sexual arousal or gratification, permits, uses or installs an imaging device to surreptitiously view a person dressing or undressing when the person has a reasonable expectation of privacy; or
- (iii) uses or installs an imaging device to surreptitiously view under the clothing of a person - commonly known as - upskirting,- or (iv) for amusement, entertainment, or profit, or to abuse or degrade the victim, permits, uses, or installs an imaging device to surreptitiously record



another person dressing or undressing when the person has a reasonable expectation of privacy.

A person is guilty of the dissemination of an unlawful surveillance image in the first-degree, a Class E Felony punishable up to 1 - to 4 years in State prison, if he or she:

- (i) publishes or sells an image that was unlawfully obtained; or
- (ii) disseminates an image he or she unlawfully obtained; or
- (iii) commits the first degree offence and has prior conviction of the first or second degree offences.

The federal Video Voyeurism Protection Act of 2004 makes it a federal crime to secretly capture images of people on federal property in situations in which they have the expectation of privacy.

3.3 Canadian Perspective on Voyeurism

In a number of Canadian cases, court has considered it relevant that persons convicted of crimes involving sexual and non-sexual violence have had a behavioural history, which included voyeurism.¹ Moreover, studies have shown that men commit most sex crimes and women and children are usually the victims.²

Another characteristic of voyeurism as a *paraphilia* is a high frequency of deviant acts *per individual*. For example, in one study of 411 men, 13% (62 men) admitted to being voyeurs and self-reported 29,090 voyeuristic acts against 26,648 victims.³ Studies suggest that voyeurs justify their behavior with rationalizations or cognitive distortions, convincing themselves, for example, that their actions do not cause any harm or that the victim actually wanted to be observed. As with other sexual disorders, voyeurs characteristically have little empathy for the victim and have an impaired capacity for emotional or sexual intimacy. The

¹See *R. v. Dickinson*, [1984] O.J. No. 100 (Ont. C.A.); *R. v. Wilson*, [1996] A.J. No. 731 (Alta. C.A.); *R. v. Deforge*, [1986] B.C.J. No. 648 (B.C.C.A.); Voyeurism was found by the court to be part of a blend of sexual disorders suffered by an accused in a successful dangerous offender application brought for sexual offences in *R. v. Johnson*, [1997] O.J. No. 2535 (Ont. C. J. (Gen. Div.)); Prior voyeuristic behaviour was accepted by the court as part of an agreed statement of facts relevant to sentencing in *R. v. A.D.R.*, [1991] N.J. No. 154 (Nfld. S.C.); *R. v. A.B.C.*, [1991] A.J. No. 1118 (Alta. C. A.) (In the latter case the court found that the voyeurism was opportunistic rather than planned); in *R. v. Currie*, [1997] 2 S.C.R. 260 the Supreme Court of Canada restored a finding that the offender was a dangerous offender. In doing so, the court accepted the evidence of the Crown expert as well as that part of the defence expert's testimony which established "the profound nature of the respondent's sexual problems" which included (in addition to a record of sexual offences) an "impulsive personality disorder and a polymorphous sexual deviation" that "includes voyeurism, heterosexual pedophilia and hebephilia and impulsive sexual aggressiveness."

²*R. v. Osolin*, (1993), 86 C.C.C. (3d) 481 (S.C.C.), at p. 521

³Abel, G.G., and J.L. Rouleau, "The Nature and Extent of Sexual Assault," in W.L. Marshall, D. and R. Laws, and H. E. Barbaree (eds.), *Handbook of Sexual Assault: Issues, Theories and Treatment of the Offender* (New York: Plenum Press, 1990), pp. 9-21, at p. 15.



risk factors for recidivism are similar to those that pertain to other sex offenders. Voyeurism as a sexual disorder manifests early in life (the average age is 15), is chronic, and tends to last a lifetime, unless treated.

3.4 Indian Legal Regime on Voyeurism

In India, the capturing, distribution and transferring of images of 'private areas' of a person's body, under circumstances where the person would have a reasonable expectation of privacy that their body would not be exposed to public view, is punishable with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. However, this does not cover instances where a person observes another in places and situations where they do not consent to being observed. The inclusion of voyeurism as an offence in the IPC would close several loopholes in the voyeurism law and hopefully be a precedent for the state to better work towards securing the bodily privacy of its citizens.

The Indian Penal Code,¹ which deals with voyeurism as – “Whoever watches, or captures the image of, a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.”

Explanation - 1 For the purposes of this section, “private act” includes an act carried out in a place which, in the circumstances, would reasonably be expected to provide privacy, and where the victim's genitals, buttocks or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the person is doing a sexual act that is not of a kind ordinarily done in public.

Explanation - 2 Where the victim consents to the capture of images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section.”

The provision seeks to protect victims of voyeurism, who have been watched, or recorded, without their consent and under circumstances where the victim could reasonably expect privacy, and where the victim's genitals, buttocks or breasts have been exposed. A reasonable expectation of privacy means that in the circumstances, whether in a public or a private place, the victim has a reasonable expectation that she is not being observed engaging in private acts such as disrobing or sexual acts. The test of reasonable expectation of privacy can be derived from similar provisions in voyeurism from the Information Technology Act.² It is particularly

¹ Section 345 AD of IPC 1860

² section 66E of Information Technology Act 2000 (amended 2008)



important because voyeurism does not necessarily take place in private places like the victims home, but also in public spaces where there is generally an expectation that exposed parts of one's body are not viewed by anyone.

The amendment to the Indian Evidence Act¹ reads, "In a prosecution for an offence under section 354, section 354A, section 354B, section 354C, sub-section (1) or sub-section (2) of section 376, section 376A, section 376B, section 376C, section 376D or section 376E of the Indian Penal Code or for attempt to commit any such offence, where the question of consent is in issue, evidence of the character of the victim or of such person's previous sexual experience with any person shall not be relevant on the issue of such consent or the quality of consent." ²According to the above provision, in a trial for sexual assault or rape the evidence supplied of a victim's previous sexual experience or her 'character' would not be admissible as relevant evidence to determine the fact of the consent or the quality of the consent.

Electronic Voyeurism

Video Voyeurism is one of the most portentous of the crime that confront us today. Security in the cyber world is one of the most sensitive issues in the gamut of cyber laws. As the internet rapidly enters the home of the common man, through computers, television, cell phones, and so on, it emerges that violation of privacy is not a threat to dot coms and experts, but also the internet community at large. While in many other countries, there are now a variety of statutes to deal with voyeuristic conduct in place that seeks to protect these inviolable rights, India is not lagging behind to check this new form of felony due to the advancement in the technology, the legislature introduced Section 66E vide the Information Technology Amendment Act, 2008 which came into force on 27 October, 2009. The Section 66E IT Act, 2008 recognizes the right to protect the human body from unreasonable and obscene intrusion by surreptitious video technology and adequately protects the individual privacy from the crime of video voyeurism which destroys personal privacy and dignity by secretly videotaping or photographing unsuspecting individuals.

4. Critical Analysis of Indian Law on Voyeurism – Where are we failing!

A 'voyeur' is generally defined as "a person who derives sexual gratification from the covert observation of others as they undress or engage in sexual activities." Voyeurism is the act of a person who, usually for sexual gratification, observes, captures or distributes the images of another person without their consent or knowledge. With the development in video and image capturing technologies, observation of individuals engaged in private acts in both public and private places, through surreptitious means, has become both easier and more common. Cameras or viewing holes may be placed in changing rooms or public toilets, which are public

¹ Section 53A of Indian Evidence Act 1872

² A similar proviso is added to Section 376 of the Indian Evidence Act 1872



spaces where individuals generally expect a reasonable degree of privacy, and where their body may be exposed. Voyeurism is an act, which blatantly defies reasonable expectations of privacy that individuals have about their bodies, such as controlling its exposure to others. Voyeurism is an offence to both the privacy as well as the dignity of a person, by infringing upon the right of individuals to control the exposure of their bodies without their consent or knowledge, either through unwarranted observation of the individual, or through distribution of images or videos against the wishes or without the knowledge of the victim.

The Indian Evidence Act is the legislation, which governs the admissibility of evidence in the different courts. In cases of rape or sexual assault and related crimes, the evidence of consent often considered is not just that of the consent of the woman in the act at that time itself, but rather her previous sexual experience and “promiscuous character”. Even though it has been widely censured by the highest court, such practices continue to dominate and prejudice the justice of victims of sexual assault and harassment. The examination of the victim’s sexual history in court is an unwarranted intrusion into their privacy through public disclosure of the sexual history and details of her sexual life, which causes potential embarrassment and sexual stereotyping of the victim, especially in a conservative, patriarchal society like in India. With the new amendments, such evidence will not be permitted in a court of law, hence, it will act as a safeguards against defendants attempting to influence the court's decision through disparaging the ‘character’ of the victim, and will protect the disclosure of intimate, personal details like previous sexual encounters of the victim.

4.1 Case Law on Voyeurism

***Maninder Kaur & Anr vs State of Punjab & Ors- 2015*¹**

In such matters the constitutional court is predominantly pre- occupied only with the life and liberty of the citizen and the safeguards afforded by law against inimical parties smarting from what their progeny did, in their perception, to shame them and then to restrain them from taking law unto their own hands. Marriage is not central to the exercise of this jurisdiction or of its legality. It is only about protection of innocent couples tied willingly together by consent and to afford them affirmative action by Court against threat to their lives, which has to be protected even if the enormity of the threat perception is churlish, or an imaginary one, which is very hard for the Court to decide. The Court must still intervene without trying to be a peeping Tom or a voyeur in private affairs as it is certainly not the final arbiter of how hearts work in private space. Therefore, a direction must go in favour of the petitioner by a Court issued by a "Save our Souls" message sanctioned and enforceable at law. Vishal Kushwah vs. State of Madhya Pradesh²

¹<https://indiankanoon.org/doc/25979201/>, visited on 12-3-2018

² <https://indiankanoon.org/docfragment/160426822/?formInput=voyeurism>, , visited on 12-3-2018



The applicant is in custody since 10.7.2015. Investigation is over by filing of charge sheet. The offence of voyeurism punishable u/S. 354 C of I.P.C is alleged. The offence is the first offence of its kind against the applicant, therefore the I.P.C prescribes maximum penalty of three years, and therefore offence is bailable and triable by Magistrate. The trial is not likely to conclude in the near future and that prolonged pre- trial detention being an anathema to the concept of liberty and the material placed on record does not disclose the applicant fleeing from justice and since the investigation is over and looking to the gravity of offence the applicant is entitled for bail.

State of Uttarakhand vs Ajam – 2017.¹ There is a disfigurement to the body of acid attacks victim. It reduces the chances of getting married and public employment. The cases pertaining to sexual harassment, stalking, voyeurism and acid burning are adjudicated within three months. Further, the Court gave a direction that cases registered under Sections 326A, 326B, 354B, 354C, 254D of I.P.C should conclude the trial within three months, and in case it is not possible to conclude the trial within three months, the Trial Court shall record cogent and sufficient reasons. The Trial Court shall show due sensitivity in the matters pertaining to the acid attacks.

The Delhi District Court by awarding the accused with a year's simple imprisonment along with a fine of ten thousand rupees. A point of interest was the characterisation of the offence of voyeurism under Section 354C of the Indian Penal Code in terms of privacy, in the latter part of the judgment. Authored by Justice Susheel Bala Dagar, the portion in question reads:

“Voyeurism is a ridiculous form of enjoyment for men but a mental torture for women. Men who indulge in such enjoyment do not seem to realize that they are infringing on the fundamental right to privacy of her body of the woman. Due to such offenders the women do not feel safe inside such places where she would usually expect not to be observed.”

Vattappara vs Sri.T.A.Unnikrishnan²

The accused was having an illicit connection with one of his relatives. The *defacto* complainant, his wife resisted that relationship. Accused has committed the offence of voyeurism. He used to take obscene photographs of the private parts of his wife on mobile phone. Petitioner is the accused (husband of the *defacto* complainant) in the Crime and the same was registered in Vattappara Police Station registered for offences punishable under Section 323, 354 (2) and 506 (i) of I.P.C. and Section 66 of the Information Technology (Amendment Act) 2009.

Conclusion

The growth of cyber-crime in India, as all over the world, is on the rise. Anybody who uses the Internet is at risk for becoming a victim of cyber-crime. Cyber space offers a plethora of

¹ <https://indiankanoon.org/docfragment/160426822/?formInput=voyeurism>, , visited on 12-3-2018

²Bail Appl..No. 7230 of 2015, Accessed from the web site:

<https://indiankanoon.org/docfragment/160426822/?formInput=voyeurism>, , visited on 12-3-2018



opportunities for cyber criminals either to cause harm to innocent people. From the above discussion, it was observed that there is no specific provision to protect security of women and children, however there are few provisions to cover some of the crimes against women in cyber space. In order to avoid the cyber-crime we should not engage in conversation with people we do not know. People on the other end of the computer may not be who they claim to be. We must keep our passwords protected and do not keep sensitive material on the computer as the hacker can access that. If anything seems out of place or wrong, contact law enforcement immediately. Indian women netizens are still not open to immediately report the cyber abuse or cyber-crime. This nature provides the offenders the chance to escape after the commission of cyber-crime. The problem would be solved only when the victimized woman then and there report back or even warn the abuser about taking strong actions. With the recent debates on women's safety, several crucial privacy and security issues have been raised, such as the criminalization of voyeurism and stalking, which is a huge boost for privacy rights of women in India, and it is hopeful that the government will continue the trend of considering privacy issues along when addressing security concerns for the state. Finally, the offence of voyeurism is not intended to capture the activities of persons who simply consume voyeuristic images. A person who produces voyeuristic images for personal use could be charged under the voyeurism scheme. Similarly, a person who receives voyeuristic images and then sends those images to others would be subject to prosecution, along with the original producer and distributor of the material. However, a person who is sent voyeuristic images and views or records them for his or her own use would not meet the *actus reus* of "views or records." It is also noted that the terms "privacy" and "video voyeurism" has still not been defined under the amended Information Technology Act, 2008. Thus, it can be concluded that the sending of an MMS capturing the private area of any person thereby violating of his privacy under the parameters detailed under the IT Act.¹ It is suggested that it is high time to brought voyeurism within the ambit of IT Act by way of prescribing penalty and punished with imprisonment for a term three years or with fine, which may extent to two lakh rupees, or with both.

¹ Section 66E of the IT Amended Act, 2008



Cyber Laws in India: Techno-Legal Challenges affecting the Enforcement

Dr. Nagarathna A.,

*Associate Professor in Law and Co-Ordinator, Advanced Centre for Research Development,
and Training in Cyber Laws & Cyber Forensics, National Law School of India University,
Bengaluru*

&

Ms. Shiyana Sebastian

Research Scholar, National Law School of India University, Bengaluru

I. Introduction

Cyber space is a borderless environment or virtual location beyond territorial boundaries and national sovereignties within which electronic activities takes place surpassing geographical limitations. Commercial activities, communication and transactions on Internet thus goes beyond territorial limits of a nation raising questions about a state's jurisdiction as well as sovereignty. As in real world, in the virtual world too there are properties, ownerships and all kinds of human transactions and communications which invite the necessity of a code of conduct. But a law without power of enforcement is meaningless. One of the main challenges affecting enforcement of laws and regulations in cyber space is absence of effective statutory provisions. In India, this code of conduct for cyber space transactions are codified as the Information Technology Act, 2000 which was further amended in the year 2008 hereinafter called as IT Act. The IT Act amended some of the provisions of our existing laws i.e. Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 mainly to facilitate e-commerce. The provisions of IPC which are amended by the IT act facilitates registration of some cyber crimes under IPC too.

Crime is generally defined as an intentional act or omission in violation of a criminal law, committed without any ground of defence or justification. Similar is also the conceptual understanding of the term cyber crime. CED [Organisation for Economic Co-operation and Development] defines cyber crime as any illegal, unethical or unauthorised behaviour involving automatic processing and transmission of data. A simple definition of cyber crime would be 'unlawful acts wherein the computer is either a tool or a target or both'. Traditional crimes such as theft, fraud, forgery, defamation, mischief, etc., become cyber crimes when the offences are committed with the help of computer, internet or its enabled services. But the conviction rate of cyber crimes in India is very poor. Existing legal framework of India even fails to define the term cyber crime. Many forms of cyber wrongs are not even expressly criminalised or dealt with under the existing law – the Indian Information Technology Act of 2000. In certain other cases law cannot be enforced properly due to the technical and other issues.



The enforcement of a law depends upon the awareness of laws among the subjects, the efficiency of law enforcement agencies, the appreciation of laws by courts of law and the remedies ensured by the laws towards accused and victims and the effect of the same in the society as a whole. But in reality, the effective execution of the IT Act still remains a dream, as the police officers, lawyers, prosecutors and Judges are not well capable to understand its highly technical terminology. The knowledge of technology is necessary to understand the possible misuse of technology and consequences in society. The law enforcement agencies as well as all the stakeholders who want to protect their data from cyber threats have to be skilled in technology to prevent cyber crimes. Moreover, the technology keeps changing day by day which is inevitable. But is it possible to change laws in accordance with change in technology? Ever since the internet became popular in India, laws in India has been developing through trial and error and imitating the laws of other countries. Some major changes were brought to IT Act in 2008 which made modifications in procedural and substantive provisions in the IT Act to combat cyber crimes. But it still remains ambiguous and not clear.

There should be clear distinction between civil and criminal wrongs in cyber space. *Mens rea* or guilty mind distinct between civil and criminal wrongs. The "act" and the "intention" of the accused must be concurrent to constitute an occurrence of offence or a crime. Hence it is a general rule that the crime is of two elements: (i) the criminal act or omission or *actus reus*; and (ii) the mental element or *mens rea*. An act without guilty mind and a mere intention to commit an act defined as a crime should not be punished. An "act" becomes an offence or a crime when it is so defined by statutory enactment or common law. Section 66 read with section 43 of the IT Act provides that there should be *mens rea* to constitute an offence. But the requirement of *actus reus* is silent in the provisions under section 43(i) of the Act. According to Section 43(i), certain actions such as destroying, deleting or altering information in a computer irrespective of consequences and certain consequences such as diminishing the value or utility of information in a computer irrespective of the action which contributed to it are punishable if committed with *mens rea*. To be guilty of cyber crime in India, a person must act voluntarily and wilfully. So the basic principle that an act will become an offence when both elements of crime such as *mens rea* and *actus reus* is neglected in the provisions. Moreover, the judiciary is vested with discretionary power to find there is any *mens rea*. So the courts have to be very cautious to take cognizance under IT Act as it largely involves claims of fundamental rights of freedom of speech and expression. In *S Khushboo v. Kanniammal*¹, Supreme Court has held that in such cases, the Magistrates should direct an investigation into the allegations before taking cognizance of the offence alleged. If you think in the line of *Shreya Singhal* case², shouldn't these provisions too be

¹ *S Khushboo v. Kanniammal*, Criminal Appeal No. 913 of 2010 on 28 Apr., 2010(India).

² *Shreya Singhal*, Writ Petition (Criminal) No.167 Of 2012 decided on 24 Mar. 2015; See also *Kartar Singh*(1994) 3 SCC 569(India).



held unconstitutional for being ambiguous? *Shreya Singhal v. Union of India*¹ is the case in the light of a series of arrests made under section 66A of the IT Act, 2008. In *Shreya Singhal v. UOI*, The supreme court held Section 66A of the Act unconstitutional for the ambiguity in its provisions. If that is the case, there are still provisions which are ambiguous in the statute as narrated above. When an act is held punishable irrespective of consequences, how can it attribute criminal intent to a person? The same way, shouldn't an ordinary person be informed what all actions are prohibited in clear terms? After all, every person is presumed to have some knowledge of the law. The clarity in legal provisions is not only beneficial to the victims but also to the accused too.

The anonymity and the borderless nature of cyber space make it more difficult to enforce the law at global level too. The lack of international harmony on the cyber crime prosecutions are clear challenges for the enforcement of cyber laws. In light of the above discussion, it is a need of the time to develop regulatory measures to address cyber crimes and to strengthen cyber laws in India. This article is divided into five parts: Part I, is the introduction. Part II is dealing with challenges of cyber laws in light of international laws. Part III deals with challenges of enforcement of Information Technology Act along with other substantive laws in India. Part IV deals with challenges of enforcement with respect to procedural aspects of cyber laws in India. Part V is dedicated for conclusion and suggestions.

II. Enforcement of Cyber laws and International Laws

Jurisdiction is an essential aspect for state sovereignty and effective judicial, legislative and administrative system. But cyber space knows no boundaries or territorial limits. Since nations assert authority on the basis of territorial nexus over individual, events and happenings occurring within its jurisdiction, cyber crimes threatens such authority of the nations and international principles of law. According to Section 1(2) and 75 of the IT Act, the Indian courts have extra territorial jurisdiction to deal with cyber crimes, but not on civil matters. These provisions have to be read along with the relevant provisions under the section 4 of IPC. It is clear from section 75 of the IT Act that the provisions of the Act is applicable irrespective of nationality of accused and that it is applicable to all offences related to computers.

Unlike India, other countries like USA and UK, the extra territoriality seems more difficult in execution as the accused may subject to different laws under different State laws. In UK, section 4 and 5 of The Computer Misuse Act, 1990 provides that it is not necessary for the cyber crime to be committed within the territory of United Kingdom so long as the offence is significantly linked to the United Kingdom. So even a legal act within other jurisdiction can become cyber crime in UK if the act is a crime in United Kingdom and it is significantly linked to it. The Police and Justice Act, 2006 brought amendments to this Act and enhanced punishments under the Act

¹ *Id.*



for committing the cybercrime. Exposing accused into a universal jurisdiction and assuming jurisdiction based on mere availability of a website is doubtful in execution. The Indian courts are of the view that a passive website, with no intention to specifically target audience outside the state where the host of the website is located, cannot vest the forum court with jurisdiction.¹

On internet transactions there cannot be a single centralised agency to regulate all the transactions. An international co-operation is necessary to curb cyber crimes effectively. There should be sharing of information, technology, and assistance for prosecution of criminals in transnational crimes. The IT Act itself is the product of following the UN Model of E-commerce. The Budapest Convention on Cyber crimes, 2001 of which India is not a signatory is a relevant international agreement on cybercrime and electronic evidence. In 2013, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), released a manual titled the Tallinn Manual on the International Law Applicable to Cyber Warfare. Though we need regulations against cyber warfare, it was widely considered as not suitable for India. In 2017, another manual called Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations was released relating to global cyber activities in peacetime. In 2011, Russia submitted to UN General Assembly an International Code of Conduct for Information Security to develop norms of behaviour in the digital space, and in revised form in 2015 by member states of the Shanghai Cooperation Organization (SCO). This document is based on a basic principle that the rights of an individual should be protected online and offline similarly. But the code of conduct concerning privacy and other fundamental freedoms led to a cold reception of the said Code. These international conventions and Codes are very much relevant for cyber security but are not acceptable for all countries including India due to its non-inclusiveness. The fading consensus on the existing international documents shows the need for more room for negotiations through multilateral treaties. The international Cooperation can also be secured by Bilateral Mutual Legal Assistance Treaties (MLAT). The cooperation of private sector and government agencies for preventing cyber crimes and enhancing cyber security is also very necessary. Such global initiatives only could develop an open, free, safe and secure cyber space. Even if there is no clear consensus on cyber sovereignty of nations, as the cyber activities cannot happen in a legal vacuum, the states should bear their responsibilities and enjoy rights for a secure cyber space. An International Convention is the best solution for transnational cyber crime challenges and it can be further strengthened by specific procedural arrangements through bilateral mutual legal treaties.

¹ In *Banyan Tree Holding (P) Limited vs A. Murali Krishna Reddy & Anr.* on 23 Nov., 2009, the court held that the mere accessibility of the defendant's website in Delhi would not enable a court to exercise jurisdiction.



III. Information Technology Act and Substantive laws in India

Cyber crimes and cyber laws:

Crime is an act which invites punishment by law. In the virtual world, some acts though contrary to morality and social order, may not be punishable by law as cyber crime is an undefined term and also it is very difficult to have a code of conduct acceptable in the virtual world beyond national jurisdictions. IT Act is not the only Act deals with cyber crimes. The Indian Penal Code also has provisions for cyber crimes of which some are triggered by IT Act and some are not. Section 81 of the Act deals with jurisdiction on the basis of subject matter. It provides that the provisions of IT Act has an overriding effect on other statutes on the subject contained therein. It also makes exception for the Patent Act and Copyright Act specifically. According to the legal maxim "*Generalia specialibus non derogant*", the general law is subjected to special law. But it does not mean that the provisions of a general statute and special statute cannot co-exist as long as they are not inconsistent to each other. In a very recent judgment, in the light of Food Safety and Standards Act, the supreme court held that there is no bar for prosecution under Penal Code merely because provisions in the FSS Act prescribe penalties.¹ If that is the case, the prosecution under IPC and IT Act should co-exist too which is a regular practice in India. But The Information Technology Act, 2000 has not defined the term 'cyber crime'. The Indian Penal Code has not even used the term cyber crime. Cyber crimes are New Generation crimes such as Computer hacking, software piracy, internet paedophilia, industrial espionage, password breaking, spoofing, telecommunication frauds, e-mail bombing, spamming, pornography, availability of illicit or unlicensed products, Credit card frauds, cyber terrorism, cyber laundering, criminal use of secure internet communications, etc. Even though IPC and IT Act are applicable to address cyber crimes, some forms of cyber crimes are not specifically addressed under either of the statutes. There is no specific provision for financial or banking fraud in IT Act or IPC which is a very rampant crime all over the world. Now a days, internet and social media facilitate cyber conspiracy to commit traditional crimes. Criminal conspiracy is dealt under Sections 120-A and 120-B of Indian Penal Code (IPC). But there is no direct provision on this point in IT Act. Moreover, hacking is a most common cyber crime which can range from minor effect to very serious effect in the society is not even included in Chapter XI of the IT Act which is a dedicated chapter for specifying penalty of cyber crimes. In India, there has been found the number of cases of cyber crimes like cyber defamation, cyber stalking and cyber harassment etc. but there is no specific definition under the Information Technology Act, 2000. In comparison of offline attempt of defamation, online defamation is more vigorous and effective. Quantitatively, the reach of a defaming comment is gigantic in online media and hence would effect the reputation of the defamed person much more than would an ordinary publication. Fraud profiles of celebrities and politicians on social media is a perfect example for

¹ 2018 (4) KHC 647 (SC)(India).



this. Cyber defamation is covered under Section 499 of IPC read with Section 4 of the IT Act. While Section 499 of IPC provides provision for defamation, Section 4 of IT Act gives legal recognition to electronic records.

It is found that a number of these types of crimes are either not registered or are registered under the existing provisions of Indian Penal Code, 1860 which are ineffective and do not cover the said cyber crimes. But sometimes the IT Act overcomes its lacking by depending on other statutes like IPC and other special statutes. For example, offence of the publication of obscene matter under Section 67 is not satisfactory under IT Act. But it can be complemented when read with section 292 of the Indian Penal Code, and provisions of The Indecent Representation of Woman (Prohibition) Act, 1987. Sometimes internet facilitates to evade laws for lack of enforcement machinery under the statutes. For example, Gambling is illegal in many countries. In India, Section 3 of the Public Gambling Act, 1867 prohibits gambling. But people offer gambling services on the Internet from countries where gambling is permitted and players from countries where gambling is illegal play and bet. Relevant provisions of the IPC dealing with cheating, criminal misappropriation or criminal breach of trust could be applied in cases of online gambling. However, there is no direct law on this point. Internet is also being misused for sale and purchase of illegal goods and services. This would include sale of narcotics, weapons and wildlife, pirated software or music and distribution of data on private persons and organizations etc. by information on websites, auction websites or simply by using email communication. Online sale of illegal articles are governed by Section 8 of the Narcotic Drugs and Psychotropic Substances Act, 1985 which prohibits sale or purchase of any narcotic drug or psychotropic substance. Section 7 of the Arms Act, 1959 prohibits sale of any prohibited arms and ammunition, whereas Section 9B of the Indian Explosive Act, 1884 makes sale of any explosive an offence. Wild Life (Protection) Act, 1972 prohibits sale of banned animal products. But when the crime is committed with the help of computer enabled services, there is no specific provision under the IT Act. Cyber stalking is an electronic extension of stalking. It involves repeated threats and harassment of a victim through e-mail, chat message or web pages. Cyber stalking involves pursuit of a victim and its movements online by posting messages on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with e-mails etc. Cyber bullying is another worse crime which has no geographical boundaries. But these offences has not specifically addressed under the IT Act. Stalking and criminal intimation, are generally dealt under IPC only. But the consequence is that many offences which are bailable under IT Act may become non-bailable when it combines with charges under IPC or other statutes. This has great impact in the society as the freedom of an accused can be limited depends upon the nature of the crime.



Cyber laws on Data Protection

The computers are nowadays most important source of preserving the personal as well as official data and personal information. Any person, authorised or unauthorised, capable of obtaining this data can make use or abuse of it. By way of amendment in 2008 Section 72A has been introduced in IT Act to cover offences regarding disclosure of information in breach of lawful contract by an intermediary. Section 72 A of the IT Act was the only resort in the absence of data protection laws in India. Section 72A and also section 72 [which imposes similar obligation on a person discharging his duty under law – such as a police officer] are the corresponding criminal provision for the civil remedy available under section 43A of the Act. In India, an institution dealing with data is subject to data protection provisions under section 43A of the IT Act and the Information Technology (Reasonable Security Practices and procedures and sensitive personal data or Information) Rules, 2011.

When the data is proprietary, intellectual property laws come into play. Section 63 of the Copyright Act, 1957 deals with the protection of proprietary data. In the case of software protection, section 65 B of the Copyright Act and section 463 to 468 of IPC are there. But there is no clear provisions for handling Intellectual property laws, domain name issues and related concerns such as cyber squatting under IT Act. For curtailing the offences of cybersquatting and phishing, generally the provisions of Trademark Act are also very relevant in addition to the provisions under section 66D of the IT Act. In *Yahoo! Inc. v. Akash Arora and another* case,¹ the issue of domain name is entitled to equal protection as trademark which is considered as the first case where an Indian Court delivered its judgment relating to domain names. In *Rediff Communications ltd. V. Cyberbooth*² case, the Yahoo judgment was once again reiterated. But the issue is some use of data which are protected as fair use under Intellectual property laws can be considered as an offence under IT Act. Though Section 81 of the IT Act clearly says that the provisions of the Act will not affect the provisions under Copyright Act, it can still stir some confusion as to application of laws.

The right of privacy is considered as a fundamental right of the individuals in almost all the countries of the world. The availability of the data in the cyber space, through hacking or by other means with capability to access, may cause the criminal infringement of privacy. It also causes the infringement of the right of privacy enshrined in Article 21 of Constitution of India. Section 28,29, 32 and 33 of the Aadhaar Act, 2016 and Sections 43A, 69A and 69B of the Information Technology Act complement each other for the protection of sensitive information. The Aadhaar Act, 2016, raised much hue and cry regarding privacy and protection of the demographic and biometric information collected for the purpose of issuing the Aadhaar number.

¹ *Yahoo! Inc. v. Akash Arora and another* , 1999 IAD Delhi 229, 78 (1999) DLT 285(India).

² *Rediff Communications ltd. V. Cyberbooth* , 1999 (4) Bom CR 278(India).



Section 43A of the IT Act provides for Compensation for failure to protect data while possessing, dealing or handling any sensitive personal data or information in a computer resource by negligence in implementing and maintaining reasonable security practices and procedures and any consequent wrongful loss or wrongful gain to any person. Rule 3 of the IT Rules enlists personal information that would amount to Sensitive personal data or information of a person and includes the biometric information. Even the Aadhaar Act states under section 30 that the biometric information collected shall be deemed as “sensitive personal data or information”, which is similar to section 43A of the IT Act. Hence the data collected under Aadhaar Act can be protected under IT Act and the agencies under UIDAI have to follow the conditions as specified in Section 43A. Chapter VII of the Act provides for offences and penalties, but does not talk about damages to the affected party. Section 37 provides that unauthorised dissemination of information under the Act to unauthorised persons shall be punishable. Section 38 to 41 prescribes penalty for offences under the Act related to data protection. Aadhaar Act has provisions for penalty but no provisions for measures for security of data and compensation. Rule 4 of IT Rules requires a body corporate to provide a privacy policy on their website and Reasonable security practices and procedures. This has to be followed by agencies under Aadhaar Act too. The prior consent rule is envisaged under Rule 5 of IT Rules. All these privacy protection provisions are not mentioned and not practiced under Aadhaar Act. The major purpose of Aadhaar is to facilitate the reach of subsidies to citizens of India. The Aadhaar Act provides that the data collected can only be used for the purpose of the Act. So the agencies under the Act have the responsibility not to share the data for any other purpose and to protect or destroy the data after the accomplishment of purpose. The Ministry of Electronics & Information Technology released a letter dated 04.05.2017 with a guideline to all Aadhaar user agencies or departments regarding Dos and Don'ts in order to prevent violation of Aadhaar Act and IT Act. It is therefore important that the bodies collecting, handling, sharing the personal information and are governed by the Aadhaar Act, must adhere to section 43A and the IT Rules 2011. However, this situation leads to ambiguity regarding interpretation and implementation of the Law. Hence there should be harmony of laws to make all the bodies under this Legislation like the enrolling agencies, Registrars and the Requesting Entities accountable under the Aadhaar Act and to protect privacy concerns. The constitutionality of Aadhaar was upheld by a recent judgment of Supreme Court in *Aadhaar Case*,¹ and held that data must be vested with the individuals all the time and consent of individuals is mandatory for collecting data and that the mandatory linking of Aadhaar for obtaining services is unconstitutional. According to Justice

¹ Justice K.S. Puttaswamy (Retd.) And Another v. Union Of India And Others, Writ Petition (Civil) No. 494 Of 2012 decided on 26 Sept. 2018.



D.Y. Chandrachud, the only dissenting judge, “Constitutional guarantees cannot be compromised by vicissitudes of technology”. This has to be in the minds of law makers.

In India, Section 66 E is inserted in IT Act, 2000 after amendment in 2008 for providing punishment for violation of privacy. This section applies to the violation of the bodily privacy of any person by three stages i.e. capture, publication and transmission. In other words, Section 66E deals with privacy issues in a very restrictive sense as it covers privacy of private parts of a person only while other states like USA and UK have specific legislations to deal with privacy issues such as the Electronic Communication Privacy Act, 1986 and the Online Privacy Protection Act, 2000 respectively. Now a new Data Protection Bill, 2018, has been introduced by which the enforcement of laws for protection of data can be improved to a large extent in India as it has implications on government and private players to protect data. The new Act is to ensure autonomy of an individual on usage of personal data and to make obligations on agencies dealing with such data to protect the same and for the establishment of a Data Protection Authority. This Act is a major step towards protection of right to privacy of individuals. The interplay of general and special laws in cyber space sometimes complements to the effective enforcement of cyber laws but sometimes can put accused to a very disadvantaged situation. This interplay of various cyber law provisions are evident in many case laws.¹ Regarding all these crimes demand clear penal provisions under IT Act.

Civil and criminal liabilities

The amendment of the IT Act in 2008 brought many changes in criminal and civil liabilities under the Act. For civil issues compensation limit has been removed from Section 43 which was only one crore rupees under IT Act, 2000. Section 43 comprehensively covers various forms of cyber civil wrongs including hacking, data theft, data destruction, etc. Further section 43A specifically deals with sensitive personal information and imposes civil liability upon person or institution who breach such privacy. In addition, section 45 imposes civil liability for wrongs that do not get covered under other express provisions of law.

Intermediary today is also expected to discharge legal obligations so as to ensure from his side contribution towards regulation of cyber wrongs on cyber space. After the amendment in 2008, the definition of intermediary has been modified and now intermediaries are made more responsible and liable towards their acts. The newly added sections 69A and 69B are very stringent towards intermediaries casting on them obligations to assist in effective implementation of the law. On the other hand, Section 67C requires intermediaries to preserve and retain certain records for a stated period. Section 69A has been introduced to enable blocking of websites by the central government. Section 69B provides powers to central

¹ See Ramesh Rajagopal v. Devi Polymers (P) Ltd, (2016) 6 SCC 310; Deepak Omprakash Gupta v. State of Maharashtra, 2016 SCC Online Bom 3514; Hanumanthappa v. CBI, (2016) 2 AIR Kant R 627; Adv. R. Mahalakshmi v. Commissioner of Police, Greater Chennai, Egmore, 2016 SCC Online Mad 4905, etc.



government to collect traffic data from any computer resource. But clearly these powers under section 69A and 69B are vested with the central government and can very well be misused. Moreover the onus of taking precautions is on the intermediaries as per the new provisions though the actual power is vested in the government agencies. Vicarious Liability is generally not applicable to criminal laws except where there is a conspiracy or common intention to commit the crime. But the IT Act followed the provisions in Negotiable Instruments Act 1881 to impose vicarious liability on companies and its officers for the offence committed by such companies or its employees by virtue of section 85 of the IT Act. This provision can be abused too since for the individual crimes like hacking without awareness of the employers, they can be still be booked under the crime which may have great impact on the reputation and profits of the company. The provision as such in NI Act is not suitable for cases of cyber crimes because while NI Act deals with debt owed by companies itself while IT Act deals with individual crimes whether instigated by the company or not. So without sufficient proof, any charge simple based on suspicion is a clear violation of legislative intention.

IV. Cyber Laws and Procedural laws in India

After the amendment in 2008, almost all penal provisions in the IT Act made offences cognizable but bailable. It also provides that cybercrimes can be investigated by inspectors. Another important power that is entertained by investigation agencies is the surveillance power which has a great implication on the fundamental right to privacy of an individual. Provisions from Criminal procedure code applies to the investigation, inquiry and trial of cyber crimes as well in addition to the IT Act.

Unlike USA, there is no specific enactment on surveillance in India other than some of the general provisions in Indian Telegraph Act for surveillance in the telecommunication networks. Monitoring Powers of the Government are given under Sections 69, 69A and 69 B of the IT Act. Section 70 of the IT Act deals with critical information infrastructure and sections 70A and 70 B of the Act deal with Nodal Agencies such as CERT-IN. Section 69 gives the central government the power to intercept and monitor any information through computer systems in national interest, permitting it to monitor any potentially cognizable offence. This will give government endless power to "intercept or monitor any information through any computer resource". Unauthorized interceptions could soon become common. This is bound to infringe civil liberties like right to privacy or right to anonymous communication with legitimate purposes.

The IT Act, 2000 has provided punishment for various cyber offences ranging from three to ten years. These are non-bailable offences where the accused is not entitled to bail as a matter of right. The amendments to the IT Act have reduced the quantum of punishment. Government has actually relaxed the laws governing some most common cyber offences which were non-bailable offences previously. Since the majority of cyber crime offences defined under the amended IT Act are punishable with three years, (except-cyber terrorism, child pornography



and violation of privacy), they shall be bailable unless otherwise provided for repeated offenders. So the chance for deletion of evidence by the accused on bail is very high, which will pose a great challenge to law enforcement agencies.

The major challenge faced by law enforcement agencies with respect to cyber crime are in the investigation, collection of evidence, production of evidence before court of law and prevention of crime. The investigation of cyber crimes is very difficult compared to traditional crimes as the culprit can be anonymous hiding in cyber space and it is very easy to delete the evidence from the computer source. But technically it is not easy to completely remove all evidence from a computer. With the help of cyber forensic experts, the deleted materials can be recovered. Computer forensics is the science and technology of finding evidences from computer systems and it involves the process of methodically examining computer system for evidence. It is technically a process for recognition, collection, preservation, analysis and presentation of cyber evidence. But the main problem is victims are reluctant to report crimes or sometime report after much delay which affects the proper investigation negatively. The difficulty in investigation of the cyber crime, the procedural complexity and lack of interest shows by police officers to attend complaints may be some of the reasons for this. The traditional way of search and seizure is difficult in cyber crimes as it may extend to other jurisdictions across the world. Section 80 of the IT Act deals with provisions for search and seizure under IT Act. Section 80 (3) of IT Act provides that the provision of the Criminal Procedure Code, 1973 shall be applicable, subject to the specific provisions as to any entry, search or arrest, made under this section. Regarding transnational crimes, the government should take initiative to enter into bilateral treaties to make effective the provisions under section 105 of CrPC for reciprocal arrangements. Time and expertise are necessary to collect evidence in cyber crimes. The collection of physical evidence such as hardware components which contains data involves search and seizure procedures. The collection of logical evidence can be through search and extract relevant data from internet, or other data base. The provisions under CrPC for registration of crime(154), power of investigation(Section 156) are applicable in cyber crimes too. But the investigating officer who is not below the rank of an inspector has to have some computer knowledge for the purpose. But the non-exposure and lack of training of Inspector level police officers to tackle cyber crimes, their detection, investigation and prosecution can be a big challenge.

The power of search, seizure and other restraints in the case of cyber crime matters are clearly violations of individual liberty and privacy. So there should be distinct provisions for considering right to privacy in civil matters and criminal matters. In the case of companies, the publication of any data confidential may cause huge loss to the company. So the procedural aspects of this area is to be given more consideration. The provisions regarding arrest without warrant(Section 41) and all the fundamental and statutory rights of an arrestee in the case of arrest have to be followed. The power of police officers for search and seizure emanates from



sections 165 and s. 100 of Code of Criminal Procedure. If the search is made in the contravention of provisions contained in the section 100 and section 165, Code of Criminal Procedure, the search will be illegal in the eye of law even if the offence committed is a grave offence. Otherwise the evidence collected by such illegal search and seizure will not be valid. Hence the provisions of CrPC have to be followed unless specifically provided otherwise by the IT Act. The collected evidence has to be filed before the court along with other reports required under section 173 Cr.P.C.

The task of collection of evidence and its presentation before court of law is a very important aspect of criminal trial. The prompt discovery, safe custody and presentation of evidence in appropriate and acceptable form is challenge in the matters of cyber crimes. The cyber criminal are far more technologically equipped to operate into the devices of computer and related storage and communication equipments. It is imperative on the law enforcing agencies to act promptly to seize the computer evidences as the images, audio, text and other data on these media are easily destroyable or alterable .

Evidence in simple words may be defined as an act or material or anything which is necessary to prove a particular fact. In India, the law of evidence is mainly contained in the Indian Evidence Act, 1872. In a civil case, the fact may be proved by a mere preponderance of evidence, while in a criminal case the prosecution must prove the charge beyond reasonable doubt. The principles of the laws of evidence by and large are the same both for civil and criminal trials, but the way of application is different. In civil cases, both has to prove their cases by placing their evidence before the court and try to prove their cases. If a party fails to prove his case, he would lose. In criminal trial it is the duty of the prosecution to bring all the evidence before the court to prove the charge and the opposite party, as a measure of defence, has to create just doubt in the prosecution evidences. Indian Evidence Act contains explicit legal rules providing significant guidance to the judges for deciding the relevancy and admissibility of evidence produced before them during a civil or criminal trial and rule out any kind of unpredictability associated with subjective assessments. The appreciation of evidence is a process which facilitates a judge to arrive at a rational conclusion.

The amendment of Information Technology Act, 2000 brought recognition of electronic documents as evidence in a court of law. The insertion of section 65 A and 65 B are the most important among the amendments which contain special provisions as to evidence relating to electronic records. The recent pronouncement of Supreme Court stating that the recording of evidence through, video conferencing is valid in law and under section 273 of Criminal Procedure Code , has an appreciable development in the field of appreciation of evidences. The appreciation of evidence is as important as gathering of evidence. Hence the awareness of judicial officers of computer technology is inevitable for appreciation of electronic evidence. Section 46 and section 48 of the Information Technology Act, 2000 provide provision according



to which the Central Government is empowered to appoint adjudicating officers who must have the experience in both information technology and legal fields for proper adjudication of any contravention of various provisions of the Act. There is also the provisions for the constitution of a Cyber Regulation Appellate Tribunal for hearing the appeals against the orders of adjudicating officers. But these provisions make it clear that the adjudications of contraventions of cyber regulations should be made by the people of specialized knowledge. The judge before whom the prosecutions and the defence lawyers are presenting and evaluating the evidences, must be technically competent to evaluate the merits of the evidences as well as the evidentiary value of the document of data produced. But in practice, it still remains a legislative dream.

In cyber crimes, a computer may be a victim as well as weapon of cyber crimes, may be an important piece of evidence in the wake of investigation of a cyber crime and appreciation of evidence during trial. The legal position was that the standard of proof in the form of digital evidence should be more accurate and stringent compared to other forms of documentary evidence. After *Anvar v. P. K Basheer and other*¹, any electronic evidence can be proved only in accordance with the procedure prescribed under section 65 B of Indian Evidence Act, 1872 which is still not followed and results in acquittals in practice.

V. Conclusion

Sometimes law falls silent due to the challenges in the digital age. The Information technology Act 2000, the major cyber law statute even after its amendment in 2008 sometimes falls into such a dormant stage due to the challenges of its enforcement. This article dealt some of such major challenges. The IT Act is applicable to cyber crimes. But a clear distinction between cyber crime and traditional crime are not possible as the life of present generation largely depends on the use of computers and technology. This article discussed the challenges of application of specific provisions under IT Act and general provisions under IPC to deal with cyber crimes. The authors are of the opinion that there should be a clarity on the point that which provision would be beneficial and applicable to the victims and accused when a crime happens, and there should be more specific cyber legal provisions where traditional penal provisions cannot address the new generation crimes. Certain provisions like electronic payments need urgent and specific attention. Clear and specific provisions on offences like cyber theft, cyber stalking, cyber harassment, cyber defamation, spamming etc could bring expedite actions for remedying it. Not only bodily privacy, but also other forms of privacy of an individual have to be defined and taken care of by specific provisions under the Act. The case laws are yet to develop in the field of Information Technology Act in India. The interpretation of various provisions of the IT Act, therefore, has to be made according to the natural meaning flowing from it. Hence the provisions of law should be devoid of ambiguity. The ambiguity in its own provisions is another challenge found in the IT Act. For the effective implementation of provisions of cyber law

¹ *Anvar v. P. K Basheer and other*, Civil Appeal No. 4226 Of 2012 decided on 18 Sept., 2014.



statutes, there should be proper checks and balances of powers given under the provisions. Therefore, the Rules should be framed under the statutory provisions so as not to misuse the power. The liability of state agencies, private agencies, intermediaries and individuals should be clearer in order to avoid such misuse of power. Though the surveillance and control over social media websites are difficult, there should be proper provisions to make the individual and intermediaries to be responsible for their activities which may have a socio-economic impact on the society. Clear provisions as to distinct and prosecute civil and criminal wrongs are necessary. The rights, obligations and liabilities of bloggers have to be properly defined. There should also be clarity of subject matter between cyber law provisions under various statutes such as Aadhaar Act, Data Protection Bill, Intellectual Property laws, etc when they come into play with IT Act. There should be clear provisions for handling IPR, domain name issues and related concerns such as cyber squatting. Cyber policing is impossible without technical knowledge. The adoption of new technologies is needed under the IT Act for ensuring cyber security. The officials who are dealing with cyber crimes should be trained in computer forensics and technologies to address the issue. There should be clarity on actions to be taken against any person committing crime outside India. Harmonisation of cyber laws in tune with global demands is needed too, and India should consider participating in international conventions and bilateral treaties specifically for preventing cyber crimes and facilitating prosecution of cyber crimes across territorial borders.

Along with specialised agencies for investigating cyber crimes, ordinary law enforcement agencies too should be trained as any police officer not below the rank of inspector has the duty to investigate the crimes. The Government agencies of Information Technology and Computer emergency response teams have to be developed further. For that purpose, India should seek international cooperation and also support governmental and non-governmental agencies to share legal and technical knowledge and expertise concerning cyber crimes. In India, the enforcement of cyber laws suffer due to namesake extra territorial jurisdiction, lack of laws addressing privacy issues, the ambiguity in law and admission of e-evidence and lack of technical potentiality and awareness among all stakeholders-victims, criminals, law enforcement agencies and judiciary. Indian cyber laws has to be modified to include more provisions which respect human rights and international principles of law. To conclude, to make cyber law enforcement more effective, there should be more efforts to distinguish between Civil Wrong and a Criminal Wrong in cyber space, there should be more training in Computer Technology, to preserve Evidence, to increase awareness of global nature of issues, and to respect the rights of all stakeholders involved in the crime.

Reference

1. ADVOCATE PRASHANT MALI, CYBER LAW & CYBER CRIMES(1st ed. Snow White Publications Pvt.Ltd. 2012)



2. Gheorghe-Iulian Ioniță & Ștefania-Diana Ioniță-Burda, *International And Regional Organizations With Attributes And Preoccupations In Preventing And Fighting Against Cybercrime And Their Main Accomplishments*, 5(2.1) JOURNAL OF INFORMATION SYSTEMS & OPERATIONS MANAGEMENT 570 (2011)
3. N.S. NAPPINAI, *TECHNOLOGY LAWS DECODED*, 110-289(1st ed. Lexis Nexis 2017)
4. Maneela, *Cyber Crimes: The Indian Legal Scenario*, 11 US-China L. Rev. 570 (2014)
5. P.K. SINGH, *LAWS ON CYBER CRIMES_ ALONGWITH IT ACT AND RELEVANT RULES* (Book Enclave, 2007)
6. Patryk Pawlak, *A Wild Wild Web? Law, norms, crime and politics in cyberspace*, European Union Institute for Security Studies, EUISS July (2017)



ROLE OF CYBER SPACE IN OPEN AND DISTANCE EDUCATION- AN ANALYSIS

Dr. S. K. Zareena

Assistant Regional Director, IGNOU Regional Centre, Chennai, Tamil Nadu

&

Dr. A. Pareeth JayaDevi

Assistant Professor, MEASI College of Education, Chennai, Tamil Nadu

Introduction:

The aim of this paper is to highlight the role of cyberspace in Distance education. Day by day, as information technologies improving, the mode of learning is changing from classroom to online. The cyberspace system can provide the real-time interaction between the remote students and the instructor just like in the classroom lecture. This paper focuses on accentuating the development and present techniques which are followed for distant education at present in India. It evaluates the role of cyberspace in open and distance education in Indian perspective. It also discusses some initiative taken in India.

Cyber Space: Meaning

Cyberspace is a virtual computer world in which an electronic medium used to form a global computer network to facilitate online communication. It allows users to share information, interact on one hand and entertain on other hand. It is a domain characterize by the use of electronics and the electro-magnetic spectrum to store, modify and exchange data via network systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computer and tele-communications without regard to physical geography. William Gibson is sometimes credited with inventing or popularizing the term by using it in his novel of 1984, Neuromancer.

Educational cyberspace is a specific part of the common cyberspace, having an educational purpose and characterized by targeted educational relationship with it. Consequently, internal relations, the educational cyberspace structure act as derived: they will be determined by its relationship with education subjects in terms of their effectiveness, rationality and safety.

The thought of interconnection of human beings through computer and tele-communications is very much utilized in improving the higher education in India through Open and Distance Education. The gross enrollment ratio of India in higher education is only 15% which is quite low as compared to developed as well as other developing countries.

For providing higher education to the highly populated country like India, the conventional mode of teaching through established formal institutions may not be sufficient. Hence Open and Distance Education is required.



Open and Distance Education

United Nations Educational, Scientific and Cultural Organization(UNESCO)'s initiatives in open and distance learning are based on its overall priority to ensure the right to education for all. While the use of distance education was given early support by the Organization, new developments in information and communication technologies, in particular the Internet and the World Wide Web have radically increased the demand for lifelong education but also provided new means to meet the demand.

The concept of Open learning and Distance Education system focuses on open access to education and training to make the learners free from the constraints of time and place and offering flexible learning opportunities to individuals and groups of learners.

- ❖ The term ODL aims to include openness and flexibility in terms of access curriculum, teaching –learning strategies and techniques, learning materials and resources, communication and interaction, support and delivery systems, students, tutors, staff and other experts management, housing and equipment and evaluation.
- ❖ ODL system used for school-age children, youth and other adults who are unable to attend in formal education sector, but have lot of interest to continue further education.
- ❖ It aims for educating the non-starters, drop-outs and people with intention to continue education.
- ❖ Open learning and Distance Education contributes in general education, vocational and continuing education, teacher education etc.,

ODL system in India:

In 1960s Open and distance learning was started in India. 34 Universities were offering correspondence education in 1980s. An exclusive University was established in Andhra Pradesh for Open and distance education in 1982 followed by the Indira Gandhi National Open University (IGNOU) in New Delhi and subsequently in Bihar, Rajasthan, and Maharashtra, Madhya Pradesh, Gujarat, Karnataka, West Bengal, and Uttar Pradesh in a decade in 1980s to 1990s.

Admission and Registration Process in cyber space

The cyber space utility is taken up in to-to for effective functioning of open distance learning. To spell the mode of utility

- We can start with website. Each of ODL institution is creating a website giving all the details of the institution, about the profile, authorities schools, divisions, institutions, partner , institutions, library, projects, blogs, sms in very beginning of the web-page.
- And the following web-pages speak specifically about admission procedures, registration details, examinations consists of internal and external examinations,



entrance examinations, other procedures to access the prospectus, e-resources for self-learning materials.

- Pages are allotted to address the students grievances, placement assistance etc.,
- The web-pages are prepared in a very attractive manner and in uses friendly mode.
- The cyber space is the known face of the institution. The learner can contact the institution through e-mail or by the tele phone.
- The institution will contact the learner through sms, tele-phone or by letter, whats-app, face book, twitter, Radio, Gyan-vani, Gyan-Dharshan, web conference, video conference and other social media.
- The advertisement for admission is given in the web-site and through e-mails to reach the prospective learners.
- The students are expected to fill the on-line application form by giving the details of name of the programme applied, medium of study, option for study centre, Father's name, address, contact details, date of birth, nationality, gender, category, social status, scholarship details (disability details, if any) qualification, fee payment in on-line mode, declaration along with scanned copies of photograph, signature previous education qualification certificates etc.,
- After the admission form is filled up the authorities of ODL institutions will scrutinize the on-line app form and inform the discrepancies to the electronically ad give the opportunity the correct the necessary details. If the corrections carried out were satisfactory then the on-line payment of fee is accepted otherwise the fee paid will be refunded through on-line banking.
- The second step for the candidates admitted is, they will be receiving identification card electronically with concerned authority's signature with specifications about name, enrolment number, address, the details of study centre with electronically attested photograph.
- Now the learner can check his or her details in the web-page regarding the programme. The registration status of the learner shows the details regarding the enrolment number, programme joined, medium of study, year of admission, duration of study, parent's name, date of birth, address for communication, study centre code, mobile number, e-mail id, and details of the subject, or courses to study to the complete programme.
- If the learner finds the any mistake in the registration details, they can inform the same for necessary rectification through e-mail. The authorities will attend to it without fail.

Availability of Study Material in cyber space

In ODL the study material is given in the two forms.

1. Self-instructional material.

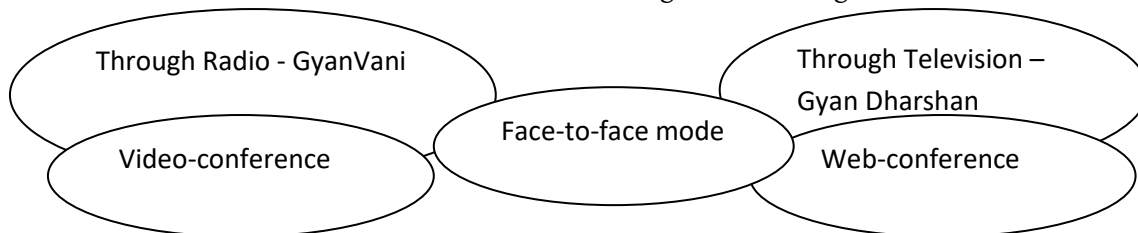


2. Study material in the form of electronic mode.

- The rural area students could not have access to internet used to receive the study material hard copy. But many urban area students are downloading the study material from the ODL institutions web-site.
- The youth are happy to use the study material in electronic form, because of its access and hassle free usage in mobile tele-phone and able to study even by travelling in roadways, railways, airways and water ways.

Facility of Contact Classes in cyber space

In ODL the contact classes are conducted through the following modes.



- In face-to-face mode, learners are attending council sessions in the study centres where the academic counselors are using PowerPoint presentations, conducting the experiments in the study centre.
- In Video conference and Web conferences, the teachers are from a different place but students will be attending from all over the country. Here the students can also interact with the teacher and get the doubts clarified. This mode is useful to attend more number of students in a shortest time with less number of teaching faculty. Another advantage with this system is the whole programme can be recorded and the student can use the recorded version and watch according to the time convenience.
- GyanVani is utilizing the media of radio for teaching the content. The learners can reach the teacher through telephone and clarify the doubts.
- In GyanDharshan, the teachers will be teaching from the studio and reaching the students all over the country. The details of GyanVani and GyanDharshan schedules are uploaded in the ODL institution web-site to facilitate the learners.

Evaluation

The evaluation procedures adopted in ODL are in the form of submission of assignments, attending the practical, projects and term-end examinations. The cyber space utilization in downloading the assignment questions from the web-site and attending on-line examinations. If the learners want to change any elective paper in the beginning of the academic year they can communicate the same to the authorities through e-mail and get it done. One great facility given to the learners is to access the on-line journals, utilize the reference material in electronic form can be utilized through the library link given in the web-site.

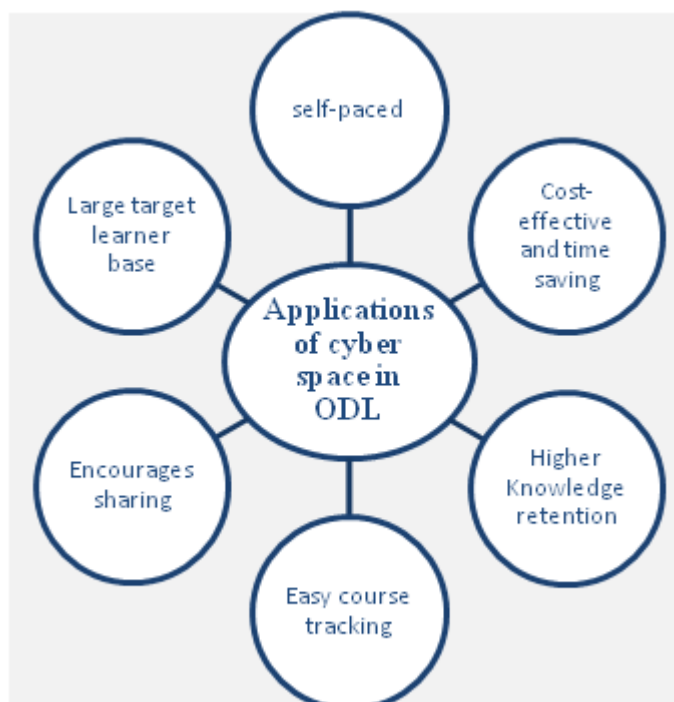


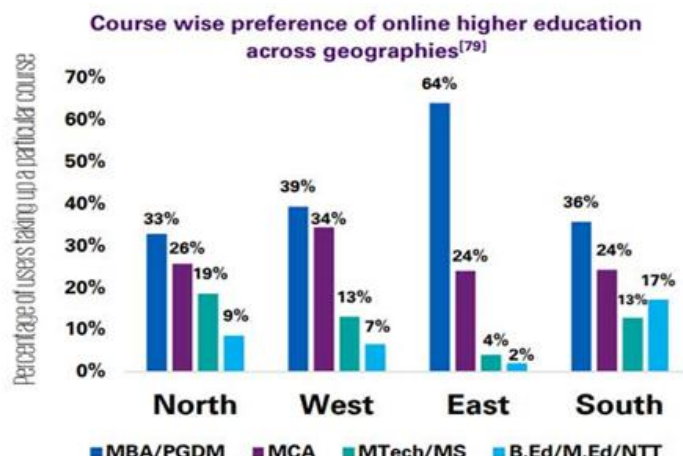
The learners can apply for examination through on-line in the ODL institution's web-page by giving the following details: enrolment number; programme code; electronic mode of payment, that is through debit card/credit card/net banking. And learner can choose any examination centre according to his or her convenience. The results of examinations will be reflected virtually in the grade card raters in the web-site facilitating the learners.

Applications of Cyber Space in Open and Distance Learning

The cyber space is utilized to the fullest in Massive Open On-line Courses (MOOCs) in which open registration, self-paced learning mechanism, creation of virtual learning community, demonstrations interaction through feedback, evaluation through quiz and activities in on-line at free of charge are available. MOOCs provides an affordable and flexible way of learning new skills to advance the carrier and deliver quality education experiences at large.

There are many on-line courses available from great universities all over the world which are all possible only through the best utilization of cyber space. It is pertinent to mention about utilization of many open educational resources through cyber space (ex: utility of second life). These services of open and distance education is fruitful with usage of social media, especially You tube, face book, twitter, whats app, instagram etc., are giving virtual experience for the learners to know about the subject, content, skills availability of resources in the world on one hand and giving an opportunity the related areas of study for further progress. Another important feature is the self-confident levels of the learners or boosted to achieve success. The key role played by cyber space in ODL is amazing. The following graph shows utilization of cyber space in education in India.





Conclusion

Cyberspace in ODL consists of common cyberspace's elements, to which educational relationships are established, aimed at achieving the objectives of education and education subjects' personal development. In this regard, almost all the resources of society in cyberspace that have the potential positive effects (scientific, educational, social, cultural, ideological, and psychological) on the subject of education can be referred to the education cyberspace. However, specialized educational portals, adapted media resources, media electronic educational resources, intended for education and subject teaching, make up the constitutive part of education cyberspace in open and distance learning.

References:

- Dr. S. Arulsamy (2010), Educational Innovations and Management (pp-159-161, 166, 174, 177-181). NeelKamal publications pvt ltd.,
- Dr. S. Arulsamy, P. Siva Kumar, (2009), 'Application of ICT in Education', NeelKamal publications pvt ltd.,
- Cohen, A. (1999). Instrumental teaching and distance learning via the Internet. Computers in Education, 49, 8-16. (Hebrew)
- Dr. K.S. Ramakrishnan (April 2008), 'Web Access and Usage Behaviour of Teacher Educators and Student teachers, Meston Journal of Research in Education.
- Dr. R. Siva Kumar, (Oct, 2008), Online classroom equipped with ICT
- Paled Alon, (2000), "Bringing the Internet and Multimedia revolution to the classroom"
- <https://www.techopedia.com/definition/2493/cyberspace>
- <https://www.learnpick.in/blog/e-learning-in-india>
- <http://www.jgrcs.info/index.php/> Saima Ghosh et al, Journal of Global Research in Computer Science, 3 (4), April 2012, 53-57



IMPACT OF CYBERBULLYING IN CHILDREN AND YOUTH- A CRITICAL ANALYSIS

Dr. V. Sowbhagya rani,

UGC PDF in Law, Sri Venkateswara University, Tirupati.

&

Prof. V.R.C. Krishnaiah (Rtd),

PG Department of Law, Sri Venkateswara University, Tirupati.

INTRODUCTION:

Cyber bullying has become an unfortunate consequence of increased online participation and interactions. Cyber bullying behaviour exhibit both short and long term effects having both significant and severe emotional and social repercussions. These repercussions include but are not limited to the following: social anxiety, depression, anger, substance abuse, eating disorders, self-harm, suicidal ideation and in some cases suicide. Bullying, no matter whether it is traditional bullying or cyber bullying, causes significant emotional and psychological distress. Cyber bullying is rife on the internet and most young people will experience it or see it at some time, can happen 24 hours a day, 7 days a week and it can go viral very fast.

According to a survey conducted by Microsoft about the global Youth found that surprisingly 53% of children have been bullied in India through different ways. This scenario is not just in India but in China, Australia, Europe and other countries. It is not just youths but people of all age groups face this problem and the biggest challenge is recognizing the bully on internet or cyberspace. The technological barriers act as a hindrance in dealing with such issues. Institutional infrastructure needs to be developed to deal with this set of bullying. In the present era of rampant growth of cyber bullying it is the biggest challenge for the legislators to deal with.

Causes of Cyber bullying:

Humans are living in the world where people bully and get bullied. Cyber bullying happens for many of the same reasons as any other type of bullying, but it may be even more appealing because it can be done anonymously. Cyber bullying is an action of using the social media technology to bully others and in main cases, it is used anonymously. By using cellphones or any other devices, such as computers and tablets to connect to the internet, a large number of individuals have been spending their time bullying other people. It may not harm somebody physically; instead it may harm them mentally.

There are two kinds of people who are likely to bully; the socially active people and the socially inactive people. It is said that bullying results in an upgrade of confidence, thinking the control is on the hands of the bully as it is also the main reason of why socially active people



may bully other people; it makes them feel powerful as it is also a way to maintain their popularity. Socially inactive people may bully other people as it is a chance to fit in and to prove that they are not weak and that they are compatible with their surroundings. Like the socially active people, bullying also makes socially inactive people feel powerful.

The exact reason of cyber bullying is unknown, but may be revenge motivated some individuals to do cyber bullying. Being victims of bullying in daily lives make them think harassing other people is only something that is natural as some people deserve to be bullied. Occasionally, it is not enough. Some say they would start to find new targets that seem to be weaker than them. Some individuals would bully only to boost their egos. These individuals simply harass others to entertain themselves and their friends who might also a bully for a high chance, not scared of getting caught as these individuals believe they will not. Attention is what some people want. There is a chance they did not gain it from their family; some are suffering from a family conflict. Most are starving for the recognition of being powerful figures. Being an arrogant one is; some bully to remind others of their social status which they believe are lower than theirs. Some do it because the people around them are doing it as well. It is said that kids see it as a trend. If one does not do it, others who are doing it would think that the ones who are not doing it are incompatible with them, another reason for them to bully the ones who are not doing it.

Types of cyber bullying:

There are many ways of bullying someone online and for some it can take shape in more ways than one. Some of the types of cyber bullying are:

- **Harassment:** It is one of the act of sending offensive, rude, and insulting messages and being abusive. Nasty or humiliating comments on posts, photos and in chat rooms. Being explicitly offensive on gaming sites.
- **Denigration:** When someone may send fake information which belongs to another person, damaging and untrue, sharing photos of someone for the purpose to ridicule, spreading fake rumors and gossip on any site online or on apps and even hear about people altering photos of others and posting in online for the purpose of bullying.
- **Flaming** is when someone is purposely using really extreme and offensive language and getting into online arguments and fights. They do this to cause reactions and enjoy the fact it causes someone to get distressed.
- **Impersonation** – This is when someone will hack into someone's email or social networking account and use the person's online identity to send or post vicious or embarrassing material to/about others. The making up of fake profiles on social network sites, apps and online are common place and it can be really difficult to get them closed down.



- **Outing and Trickery** is when someone may share personal information about another or trick someone into revealing secrets and forward it to others. They may also do this with private images and videos too.
- **Cyber Stalking** is the act of repeatedly sending messages that include threats of harm, harassment, intimidating messages, or engaging in other online activities that make a person afraid for his or her safety. The actions may be illegal too depending on what they are doing.
- **Exclusion** is when others intentionally leave someone out of a group such as group messages, online apps, gaming sites and other online engagement. This is also a form of social bullying and a very common.

The worst thing about social networking sites and messaging apps is that anything nasty posted about you can be seen by lots of people and these posts can go viral very fast and be shared by so many people within minutes in some cases.

Impact of cyber bullying on adolescents:

Cyber bullying has been conceptualized as a stressor. It involves hurting someone else using information and communication technologies. Like any other type of bullying, the effects of cyber bullying are somewhat the same. For people who are doing cyber bullying, a bad reputation in the future is waiting for them if they get caught. Since cyber bullying is also an action of bullying, there is a law for it and the victims may report the case if they have enough proof. As for the ones who develop cyber bullying, they become stressed. It would lead them to do negative things and one of them is abusing alcohol intakes or even drugs. Teenagers would skip school as they are unwilling to attend it and meet people, feeling it is tough to communicate, instead, others might laugh and pick on them. They start to doubt everyone, accusing and judging people one by one. They would lock themselves in their room or worst, they would try to attempt suicide.

For many cyber bullying affects their everyday lives and is a constant source of distress and worry. With mobile technology being so freely available it is an ongoing issue and one that is relentless. Not only does it go on after school, college or work has finished, but it then carries through into the next day and the cycle continues. It has been well documented that cyber bullying has resulted in tragic events including suicide, and self-harm and clearly, more needs to be done in order to protect vulnerable children and adults from online bullying.

Anti Cyber bullying laws in India:

Anti-bullying laws in India have been enacted to eliminate bullying in any form in different spheres like bullying at workplace, schools, cyberspace etc. The Bar Association of India gave its definition as, "Bullying means systematically and chronically inflicting physical hurt or psychological distress on one or more students or employees. It is further defined as



unwanted and repeated written, verbal, or physical behaviour, including any threatening, insulting, or dehumanizing gesture, by a student or adult, that is severe or pervasive enough to create an intimidating, hostile, or offensive educational environment; cause discomfort or humiliation; or unreasonably interfere with the individual's school performance or participation; and may involve but is not limited to: teasing, social exclusion, threat, intimidation, stalking, physical violence, theft, sexual, religious, or racial harassment, public humiliation, or destruction of property.”.

In **Vishaka v. State of Rajasthan** the Supreme Court first time dealt with issue of bullying and it laid down certain guidelines for the protection of woman employees from sexual harassment. But it only dealt with bullying against men at workplaces. Further, there is a need to consider different types of bullying at workplaces. In the west bullying at workplace is recognised as violence in workplaces. Bullying can be in different subtle forms like invalid criticism, exclusion, false allegations, constant bantering, humiliation or unnecessary written warnings.

In India a worker can seek redressal under different provisions provided under the constitution of India, IPC, and C.P.C. The Indian Constitution under various articles provides labor rights. Though not in evident form but indirectly various articles protect the labour rights for ex, Article 14 of the Indian Constitution lays down the concept of Equality before law. Right to life includes protection of the health and strength of the worker is a minimum requirement to enable a person to live with human dignity. The right to human dignity, development of personality, social protection, right to rest and leisure are fundamental human rights to a workman assured by the Charter of Human Rights, in the Preamble and Arts.38 and 39 of the Constitution.

There is no separate legislation in India to deal with bullying at school level. Bullying is prevalent at school level in India, especially in boarding schools. However in 2015 HRD ministry directed CBSE schools to form anti-ragging committees at school level also putting severe punishments to students. UGC has laid guidelines to all the colleges across the country to follow anti-ragging rules in their respective universities and the universities which do not abide by such rules would be bring to task and even UGC could forfeit their recognition. The government of India enacted special regulation to curb bullying at higher education institutions – “UGC Regulations on Curbing the Menace of Ragging in Higher Education Institutions, 2009”. A student may also have criminal liability under different sections of the criminal procedure code of India.

Conclusion:

Cyber bullying is a great danger to the society. It causes harm to people and results negatively for, both, the bully and the victim. It is said that cyber bullying is a serious worldwide issue and that it needs to be resolved. If they cannot do cyber bullying anonymously, they will go as far as



they will face claim other people only to do cyber bullying. However there is a dire need for a specific legislation as it would bring clarity on different legal aspects of bullying, ease the judicial process as well lead to better working environment.

It is important to take a proactive approach. Routine screening techniques can be developed to assist in uncovering the harm endured through cyberbullying to help support adolescents recovering from associated trauma. Finally, the study findings described above also suggest a strong need for comprehensive, school-based programs directed at cyberbullying prevention and intervention. Education about cyberbullying could be integrated into school curriculums and the community at large, for example, by engaging adolescents in scholarly debates and community discussions related to cyberbullying legislation, accountability, and character.

However there is a dire need for a specific legislation as it would bring clarity on different legal aspects of bullying, ease the judicial process as well lead to better working environment.

Reference:

1. <https://english.binus.ac.id>
2. *Beat Bullying Virtual Violence II report commissioned by Nominet Trust* <http://archive.beatbullying.org/dox/media-centre/news-archive/Feb%202012/Virtual-Violence-II-The-Real-Impact-Of-Cyberbullying.html> *Ditch the Label* <http://www.ditchthelabel.org/cyberbullying-statistics/>
3. Vishakha Vs State of Rajasthan , AIR 1997 SC 3011.
4. "Anti-bullying laws in India" Bar Association of India, 2015, < <https://www.indianbarassociation.org/wp-content/uploads/2015/11/Anti-bullying-laws-in-India.pdf>> Accessed on 16 April,2017.
5. Section 2 UGC Regulations on Curbing the Menace of Ragging in Higher Education Institutions, 2009.
6. <http://www.manupatra.com/roundup/374/Articles/Right%20to%20dignity%20at%20work%20place.pdf>
7. <https://www.emeraldinsight.com>
8. <https://www.stopbullying.gov>
9. fundforcivility.org
10. <https://www.psycom.net/effects-of-bullying>
11. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4126576/>



STATUTORY PROVISIONS ON PREVENTION OF CYBER CRIMES- INDIAN

PERSPECTIVE

Ms. Sofiya K.,

Assistant Professor,

School of Law, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu.

INTRODUCTION:

India is among those countries that have made tremendous impact in the global IT market. Contribution of software exports and IT enabled services, including Business Process outsourcing from foreign countries, is poised to contribute significantly to the national economy. A study carried out by Nasscom¹ estimates that IT and ITES exports will account for more than 30 percent of all foreign exchange earnings by 2008 and the IT industry will contribute to 25 percent of incremental GDP growth between 2002 and 2008. Similarly, a report named, "Digital Dragons" by Boston Consulting Group estimates that India will have 35 million Internet subscribers by 2004 end. The number of computer and internet literates are also growing exponentially in India, thanks various factors including introduction of computer training in the school curriculums.

Let us now analyse in detail the provisions relating to cybercrimes contained in this Act.²

INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 (hereinafter referred to as the 'Act') was passed by the Parliament to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce" or "e-commerce" in short. The Act also carry out necessary amendments in the Indian Penal Code 1860, the Indian Evidence Act, 1872, the Banker's Books of Evidence Act, 1891 and the Reserve Bank of India Act, 1934 for facilitating legal recognition and regulation of such commercial activities..

The Indian Act is mainly based on the UNCITRAL Model law on Electronic Commerce.³ The UN General Assembly Resolution adopting this Model law also call upon members to give favourable consideration to the said Model law when they enact or revise their laws, to ensure uniformity of the law across the globe. The focus of the Model law is on the need for uniformity of national laws applicable to alternatives to paper based methods of communication and storage of information adoption of reliable electronic records for efficient delivery of government services

¹ 2002 Nasscom-McKinsey study, cited in www.nasscom.org.

² See Dr. Bakshi, P.M. et al, Hand Book of Cyber and E-Commerce Laws, Bharat Publishing House (2001), New Delhi; Na. Vijayashankar, Cyber Laws For Every Netizen In India

³ UNCITRAL Model law on Electronic Commerce with Guide to Enactment



in the member states. It acts as a starting point for identification and discussion of areas where the law could be updated to consider new technology, as well as including certain internationally settled provisions for dealing with those issues.

OFFENCES AND PENALTIES

Though, the focus of the Act is not on cybercrimes as such, the Act defines certain offences and penalties that deal with acts and omissions falling under the term cybercrimes. Chapter XI of the Act deals with offences and Chapter IX deals with penalties and adjudication. Chapter IX brings a welcome change in the minds of law makers as, may be for the first time, Indian Parliamentarians have come out of their obsession with the idea of "criminalisation" as the sole means of regulating human conduct and upholding societal peace and tranquillity¹ and introduced civil liabilities as an alternative. In view of the nature of subject matter involved, the process of adjudication is not left to the hands of regular Civil Courts but entrusted to Adjudicating Officers to be specially appointed for this purpose.

performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

From the above it is clear that almost all the cybercrimes in which computer system or network is a target can be brought under the purview of this Section. Without attaching any criminal liability, the Section makes the offender to compensate any loss or damage that might have been caused by him to the victim.

Penalty for Failure to Furnish Information, Return etc.

Section 44 of the Act provides that if any person who is required under this Act or any rules or regulations made there under to-

- furnish any document; return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
- file any return or furnish any information, books or other documents within the time specified there for in the regulation fails to file return or furnish the same within the time specified there for in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
- maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

¹ For details, See Criminalization -Does Legitimacy Matter? Dr. Joga Rao, S. V., in Current Issues in Criminal Justice and Medical Law:



Residuary Penalty: Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.¹

An Adjudicating Officer appointed under the Act alone can adjudicate on these penalties or compensation has to take the following factors into account:²

The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default.

The amount of loss caused to any person as a result of the default. The repetitive nature of the default.

Offence of Obscene Publication: Section 67 makes publishing of any obscene information in electronic form an offence punishable under the Act. It provides that 'Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstance, to read see or hear the matter contained or embodied in it, shall be' punished with imprisonment and with fine.

Publication for Fraudulent Purposes

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which extend to one lakh rupees, or with both.³

No steps to combat Internet Piracy: Violation of copyrights has become rampant with the advent of Internet. Violations of intellectual property rights and piracy in the cyber space are expected to have far reaching effects on the development of human knowledge itself. However, the Indian IT Act failed to look into these aspects and tackle the menace.

Lack of International cooperation: It is an acknowledged fact that isolated national efforts cannot curb cybercrimes because it acts without any regard to physical boundaries. Though the Act proposes to apply its provisions beyond the territorial limits of the country, it is silent as to how the same is proposed to be achieved. Unless there are concrete steps towards international cooperation in combating terrorism, it is not possible to deal with acts committed over Internet by aliens. The Act fails to address this issue in the tight of possible need for extradition of other nationals to stand trial for offences committed under the Act.

¹ Section 45 of the Information Technology Act, 2000

² Section 45 of the Information Technology Act, 2000

³ Section 74 of the Information technology Act, 2000



ROLE OF JUDICIARY

The application of the Information Technology Act rests with the courts. It is a settled principle that the interpretation of a provision of law relates back to the date of the law itself and cannot be prospective from the date of the judgment because concededly the court does not legislate but only gives an interpretation to an existing law.

"A statute is an edict of the legislature. The language employed in a statute is the determinative factor of legislative intent. Words and phrases are symbols that stimulate mental references to referents. The object of interpreting a statute is to ascertain the intention of the legislature enacting it".¹

It is for the judiciary to ascertain the intention of the legislature behind the Act. The observation that the judges lack that 'technological temperament' to do justice with nuances and subtleties of information technology law is based on a narrow premise. It is true that the information technology law is different from other branches of law in the sense that it is 'dynamic' rather than static. For example, information technology law has been able to recognize the computer as a 'weapon of offence' as well as a 'victim of criminal'. This could not be said for a revolver, pistol or knife -they have always been identified as 'weapons of offence' but never as 'victim of crime'.

Further, the question that with the easier availability and wider circulation of the US case law, the judiciary in India might be tempted to use and apply the law principles established by the US courts. This threat is very real. However, one must understand that with Indian case law still in infancy, the litigants would have no other option but to resort to the US case law. In such a scenario, it is for the judiciary not to get swayed by the doctrines propounded by the US courts at the cost of already established national law principles.

The Act, though technical in content is easily understandable, if one takes into account the accompanying Information Technology (Certifying Authorities) Rules, 2000 and Information Technology (Certifying Authority) Regulations, 2001.

Assimilating Technology

The fact is, that judiciary has always been able to assimilate technology and as the Supreme Court has observed in *SIL Import. USA v. Exim Aides Silk Importers*², the need of the judiciary to interpret a statute by making allowances for any relevant technological change that has occurred.

In *Grid Corpn. of Orissa Ltd. v. AES Corpn*³, it was held by the Supreme Court that " when an effective consultation can be achieved by resort to electronic media and remote conferencing, it is not necessary that the two persons required to act in consultation with each other must

¹ *Institute of Chartered Accountants of India V. Price Waterhouse*, (1997) 6 SCC 312

² (1999) 4 SCC 567

³ (2002) 7 SCC 736



necessarily sit together at one place unless it is the requirement of law or of the ruling contract between the parties.

Similarly in *State of Maharashtra v. Dr. Praful B. Desai*¹, it was held that "Video conferencing is an advancement in science and technology which permits one to see, hear and talk with someone far away, with the same facility and ease as if he is present before you i.e. in your presence. In video-conferencing both parties are in presence of each other. Thus it is clear- that so long as the accused and/ or his pleader are present when evidence is recorded by video-conferencing that evidence is being recorded in the "presence" of the accused and would thus fully meet the requirements of Section 273 of the Criminal Procedure Code. Recording of such evidence would be as per "procedure established by law".

Thus the Supreme Court approves of the principle of updating construction, i.e. law must constantly be on the move adapting itself to the fast-changing society and not lag behind.

CONCLUSION

Reliance on terrestrial laws is an untested approach. Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cybercrimes. The majority of countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in court. Weak penalties limit deterrence. The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects. Self-protection remains the first line of defence. The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.⁴ A global patchwork of laws creates little certainty. Little consensus exists among countries regarding exactly which crimes need to be legislated against. Figure 2 illustrates the kinds of gaps that remain, even in the 19 countries that have already taken steps to address cybercrimes. In the networked world, no island is an island. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cybercrime will be complicated.

BIBLIOGRAPHY

1. http://shodhganga.inflibnet.ac.in/bitstream/10603/7829/19/19_summary.pdf
2. http://shodhganga.inflibnet.ac.in/bitstream/10603/130487/9/09_chapter%204.pdf
3. <https://www.pwc.in/assets/pdfs/publications-2011/economic-crime-survey-2011-india-report.pdf>
4. <http://www.legalserviceindia.com/article/l146-Cyber-Crime-And-Law.html>
5. <https://www.civildserviceindia.com/current-affairs/articles/types-and-prevention-of-cyber-crime.html>
6. https://www.researchgate.net/publication/262388740_Latest_Face_of_Cybercrime_and_Its_Prevention_In_India

¹. (2003) 4 SCC 601



**VIOLENCE AGAINST WOMEN IN CYBER INFORMATION SUPER HIGHWAY IN INDIA- A
LEGAL ANALYSIS**

Ms. Vijayashri V.,

*Assistant Professor, School of Law, Sathyabama Institute of Science and Technology, Chennai,
Tamil Nadu.*

Introduction

Cyber violence, an online behavior that leads to threat against the well being of an individual or group physically and mentally. Globally cyber violence is undoubtedly the new emerging form of violence and a most severe issue challenging women's dignity, security and privacy. In country like India, it is a serious threat to women where cloud technology facilities are widespread but legal awareness is low. There are billions of people who frequent the cyberspace everyday be it for professional, personal or social reasons. Almost every second household has access to the internet. With nearby two billion internet users worldwide there are greater opportunities to entrap new victims, including women and children. New information technologies are being used to commit heinous crimes.¹ Recently Department of justice statistics in US reported that 850,000 American adults- mostly women are targets of cyber-stalking each year and 40% of women have experienced dating violence delivered electronically. Pew Research Center's recent study found that 40% of adult internet users have experienced harassment online, with young women enduring particularly severe forms of it².

Different forms of cloud based offence against Women:

1. Cyber Stalking

Exponential advances in the field of information technology have led to easy victimization. Stalking according to the dictionary means to pursue or approach, prey stealthily. Cyber stalking is the stalking of any person online. In case of cyber stalking of women it means that the stalker follows her all over the net be it chat rooms, social networking websites and make life hell. There have been cases of cyber stalking which have led to cases of rapes, acid attacks and in many extreme cases murder and robberies. Cyber stalking or technology aided stalking has only been recently been recognized as crime. Internet predators have easy access to victims through facebook.com and myspace.com. Since very little empirical work has been done in this field it is not easy to draw statistics. Many women have to live in constant fear because of being stalked online by men who are sick.³

¹ G. Rathinasabapathy and L. Rajendran, "Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology (2007).

² https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Molly_Ghosh.pdf

³ Dr.Astha Bhanot, Gender Violence, Pointer Publications, Jaipur (2013) pg.26.



There are two types of cyber stalking:

- Online cyber stalking starts on the net and stays online.
- Cyber stalking starts on the net and continues offline where the stalker manages to get the woman's phone number or address and then troubles her.

Cyber stalking via technology includes:

- Sending threatening or unwanted emails, Instant messages (IM), beeper messages or cell phones text messages.
- Using a person's email address to subscribe him/her to multiple lists or to purchase goods/services in his/her name.
- Stealing a person's online identity to post false information. Sending misinformation to chat rooms, using net groups or lists to humiliate someone and/or encourage other group members to harass another individual.
- Posting a person's demographic information or photograph on pornographic sites.
- Accessing, monitoring and manipulating a person's computers while he/she is online.
- Accessing bank accounts, student's registration, telephone accounts and other personal data available online.
- Developing a website in 'tribute' to a person.
- Compiling online demographic information with intent to harass, threaten or harm a person with online/ offline
- Tracking a person through illegal wire tapping, caller identification, cameras, global positioning systems or other tracking devices.¹

2. Cyber Bullying

Bullying means systematically and chronically inflicting physical hurt or psychological distress on one or more persons.

Cyber bullying can be in different forms, for example:

- Posting any kind of humiliating content of the victim.
- Hacking the victim's account.
- Sending or posting vulgar messages online.
- Threatening to commit acts of violence.
- Stalking by means of calls, messages, etc..

¹ Harvey, D "Cyber stalking and Internet Harassment: What The Law Can Do" available on GJRIM Vol 4, No 1, June 2014 46 http://www.netsafe.org.nz/Doc_Library/netsafepapers_davidharvey_cybErstalking.pdf



The Ryan Halligan Case of Vermont (2003)¹ was the first case that dealt with the issue of cyber bullying in which the defendant was not held liable for cyber bullying because of criminal law could not be applied in that matter.

3. Harassment through E-Mails

Harassment through e-mails is no different from harassment through mails. In this women are threatened, blackmailed, bullied and cheated by emails. Men make fake email ID's and blackmail women by sending them their morphed pictures and threaten them to make it go viral if the women do not give in to their demands. There are spam mails that are sent to women and they contain viruses and worms like Trojan, love bug etc. There are some viruses that can attack the computers and extract all the personal details stored in it. People also tamper with the computer source code which is again a copyright violation.

4. Harassment by making Fake IDs

Another form of cyber crime that is on the rise lately is wherein men make fake id's of the woman concerned on social networking sites or make their fake mail accounts and the use morphed pictures which they post on the net or send through the email account to any number of people.

5. Online Pornography

Pornography in any form is a problem for women and children. There are a large number on porn sites on the net. These sites thrive on internet traffic. Many times women are not even aware of the fact that their photographs are on such sites. A large number of cases have been reported where people have morphed and doctored pictures of women and put them on porn sites. Pornography is a systematic practice of exploitation and subordination which dehumanizes women.

6. Misuse of Social Networking Sites

Now-a-days a large number of cases are reported in the police station everyday where the women are harassed to such a point by men who have morphed their pictures and made fake id's in their name and put up all their personal details on the net. Cases have been reported that men have put the woman's phone number on the net and she has been harassed by perverts. Many times people post fake photos on the social networking sites and link it to porn sites. They also post the girl's phone number and she is constantly harassed by men who are in access to the numbers.

Fraud on Dating Websites

Men on the prowl look for vulnerable women who are looking for love and are easy target of such people. They start by befriending the female and extracting all their personal details. There have been innumerable cases where women have met guys on dating sites and then have been raped and in worse cases murdered by them. Dating websites are a boon for the

¹ <https://blog.ipleaders.in/anti-bullying-laws>



psychopaths. Women fall easy prey to these psychopaths and are lured into a vicious web wherein they fall for them and give them all their personal information. Serial Killers also frequent the web as they can hide in the anonymity and it is not easy to track them down. Very rarely are these psychopaths caught.

E-Mail Spoofing

E-mail spoofing is email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Because core SMTP doesn't provide any authentication, it is easy to impersonate and itself into the person's computer triggers the virus.¹ Any mails sent forward to the other person's to whom the mails are sent. A worm can employ various methods of transferring the data.

Some Reported Cases on violence against women in online platform:

1. Manish Kathuria Case²

There is a case of Mrs.Ritu Kohli. She complained to the police that a person was using her identity to chat over the internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days. She also complained that the person was chatting on the net using her name and giving address and phone number and was talking in obscene language. Mrs.Kohli received about 40 such calls in the span of 3 days from places like Kuwait, Cochin, Bombay and Ahmedabad. Delhi police traces the IP addresses to a Manish Kathuria. He pleaded guilty and was arrested under section 509 of the IPC nothing in the IT Act.

In June 2000, a man was arrested by the Delhi Police for assuming the identity of ex- employer's wife and distributing her phone number. When the victim reported to the police that she was getting obscene calls in the middle of the night the police located the accused in the online chat room and then traced him by the telephone line used by him to access the internet.

2. A Dubai based NRI was lured by an anonymous man on the internet who after winning her love started blackmailing her. He also sent fake copies of the love letters to her friends. Charges were framed under section 292, 389, 420, 465, 467, 468, 469, 474 IPC and section 67 of the IT Act.

3. A Company's employee started sending derogatory, defamatory and obscene emails about the company's female Managing Director. The emails were anonymous and frequent and were sent to many of the company's business associated to tarnish the image and goodwill of the Company. The accused was later identifies by hiring a Private Computer Expert. Delhi High

¹ <https://blog.malwarebytes.com/cybercrime/2016/06/email-spoofing/> retrieved on 02/10/2016.

² P Shah, Cyber stalking & the Impact of its Legislative Provisions in India, <http://www.legalindia.in/cyber-stalking-the-impact-of-its-legislative-provisions-in-India> (Last visited on 02/10/2016).



Court granted an injunction and restrained the employee from sending, publishing and transmitting emails which were defamatory to the plaintiffs.¹

4. Some unknown persons had created an email id using the name of a lady and using her email id to post messages on five web pages describing her as a call girl with her contact numbers. Investigation was carried on the Chennai Police where the IP address and the ling details obtained from ISP were traced to two cyber cafes in Mumbai. Complainant received that she had refused a former college mate who had proposed to marry her. The police arrested this person and on examining his sim card found the complainant's number and the owner of the cyber café also identified this man. A charge sheet was filed U/S 67 of the IT Act 2000, 469 and 509 IPC. The accused was sentenced to 2 years of rigorous imprisonment. (*State of Tamil Nadu v. Suhas Khatti*, Egmore, Chennai 2004)²

5. Criminal enterprises benefit from the relative anonymity that the internet provides. With the strategic use of ISP by the criminals it becomes very difficult for the law enforcement to tackle them down as they relocate their ISP when they come to know that some law enforcement agencies are tracking them. These criminals sometimes work alone and in some cases they work in gangs. The major source of online exploitation is images of women where individuals pay some fee to access these sites. Other platforms are image-sharing sites, free hosting platforms and hacked websites. The less formal peer to peer networks do not leave a money trail and so it becomes difficult to track them down.

International and National Laws against Cyber crime.

At the international level Article 6 of Convention on the Elimination of all Forms of Discrimination against Women (CEDAW)³ convention urges States Parties to take all appropriate measures, including legislation, to suppress all forms of traffic in women and exploitation of prostitution of women. Beijing Declaration of women also highlighted the issue of technology and women. Declaration pointed out that the continued projection of negative and degrading images of women in media communications – electronic, print, visual and audio – must be changed. Print and electronic media in most countries do not provide a balanced picture of women's diverse lives and contributions to society in a changing world. In addition, violent and degrading or pornographic media products are also negatively affecting women and their participation in society.

¹ The Times of India, Dec 18 (2010) "Cyber defamation increasing in India available on http://articles.timesofindia.indiatimes.com/2010-12-18/security/28256203_1_cyber-defamation-blog-sites-mega-housing-project

² The case of *Tamil Nadu v Suhas Katti* is worth mentioning for the fact that the conviction was successfully achieved within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial is applaudable.

³ <http://www.un.org/womenwatch/daw/cedaw/> retrieved on 02/10/2016.



In India the term 'pornography' when used in relation to an offence is not defined in any statutes in India but the term 'obscenity' has been effectively explained in two statutes in India, and these legislations prescribe that 'obscenity' in certain circumstances constitutes an offence.¹ These legislations are

- The Indian Penal Code, 1860 (IPC) and
- The Information Technology Act, 2000 (IT Act)

Section 292 of the IPC comprehensively sets out the circumstances in which 'obscenity' and/or any 'obscene' material is an offence. According to section 292, "Whoever sells, let to hire, distributes, publicly exhibits ; Imports, exports or conveys and obscene object; Takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects ; Advertises or makes known by any means ;Offers or attempts to do any act which is an offence under section 292.

Section 292 also sets out the purposes under which obscenity is not deemed to be an offence and these are when any such material is used for interest of science, literature, art or learning or other purposes of general concern and in any Ancient Monuments and Archaeological Sites and Remains Act 1958 or in any temple, or on any car used for the conveyance of idols.

From a plain reading of Section 292 of the IPC it appears that if a person is in mere possession of the obscene material for his personal use without any intention to perform any of the purposes specified in section 292 it may not be an offence under section 292. In the case of Jagdish Chawla & Others v. The State of Rajasthan²

The accused was caught viewing an obscene film on the television with the accused was caught viewing an obscene film on the television with the help of a VCR which along with the cassette was seized and a case under section 292 of the IPC was registered. The accused filed a petition in that simply being in possession of a blue film could not make a person guilty under section 292 unless it was further proved that the purpose of keeping the same was selling or letting it on hire. However it would be prudent to be aware that a prosecution may lie for mere possession of obscene material which may be for his own personal use, actually aids and abets the publication, sale, hire, distribution etc of the obscene material, which is an offence under section 292. And under section 111 of the IPC, the abettor is held to be equally guilty of the offence which he has abetted provided it is proved that the offence is a probable consequence of the abetment.

Section 67 of the IT Act lays down the law that obscenity is an offence when it is published or transmitted or caused to be published in any electronic form. The expressions, 'publishing' or 'transmission' have not been specifically defined under the IT Act, but the commentaries suggest that 'publishing means making information available to people'.

¹ Law, Technology and Women: Challenges and Opportunities, Reference Press, New Delhi [2010], Pg.206.

² <https://indiankanoon.org/doc/170577355/> retrieved on 02/10/2016.



Transmission may be addressed to an intended recipient for his personal use. But that is not relevant. The act of 'transmission' is sufficient to constitute an offence under section 67 of the IT Act.

Therefore if any obscene material is published or transmitted in any electronic form it is an offence under section 67 of the IT Act. The transmission' and not mere possession of obscene information is an offence. The provisions of section 67 of the IT act are therefore similar to section 292 of the IPC where mere possession of the obscene material for one's own personal use may not be construed as an offence, However, it would be advisable to be cognizant of the fact that the prosecution can take a plea of abetment in a case of mere possession.

In the context of cybercafés in particular, if a customer downloads any obscene material for his personal viewing on the terminal assigned to him and this fact is known to the owner of the cybercafé would be liable under section 292 of the IPC read with Section 67 of the IT Act. Provided however, if it is established that this act was without the knowledge of the owner of the cybercafé it could be difficult for the prosecution to sustain its plea under section 292 and section 67 of the IT Act.

The law relating to the liability of cybercafé owners under these provisions of the IPC and the IT Act is not very well settled and therefore open to subjective interpretation. To mitigate liability and to avoid possible criminal prosecution the cybercafé owners could perhaps make an attempt to take protection under section 79 of the IT Act which absolves 'intermediaries', who only provide access to content but do not provide content itself, by extending the argument of intermediaries to cybercafés. The grounds of defense could be also made stronger by setting up a mechanism whereby the customers are prevented from accessing any obscene websites and disclaimers are displayed prominently informing customers that obscenity is an offence which is punishable with imprisonment and that despite the warning, if customers still view such websites, they will be personally responsible and not the owner of the cybercafé.

Under the circumstances, the law as it stands on obscenity with regard to the liability it imposes on the owners of cybercafés is certainly not free from doubt and casts an onerous obligation on them to successfully defend a prosecution under the relevant provisions of the IPC and the IT Act. However, if certain precautions are observed such as establishing mechanisms which block such websites and displaying the disclaimers as suggested above, prominently, at least may help in providing a good defense. Regarding the punishment if we analyze the sections under 292 of the IPC for the first conviction a term of imprisonment (simple or rigorous) which may extend to two years, and with fine which may extend to two thousand rupees, and in the event of a second or subsequent convictions, with imprisonment (simple or rigorous) for a term which may extend to five years, and also with fine which may extend to



giver thousand rupees. The punishment for an offence under Section 67 of the IT Act is on first conviction with imprisonment (simple or rigorous) for a term which may extend to one lakh rupees and in the event of a second or subsequent convictions with imprisonment (simple or rigorous) for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Conclusion

In this Age of information the 'virtual world' reigns supreme and it shapes our political, social and cultural outlook. Online abuse does not stay limited to cyberspace only. Shying away or going offline will not be able to solve the problem. Law enforcement agencies have to realize the gravity of the situation and frame laws accordingly and they have to realize the fact that the victims of online exploitation must live with their abuse for the rest of their lives. The whole scenario of cyber victimization is very complex and in the absence of empirical data it becomes very difficult to prove it. Cyber victimization is a violation of the fundamental rights and is gender harassment. The Information Technology Act still needs to be modified since it does not specify any crime specifically as against women and children.

Bibliography

1. Law, Technology and Women: Challenges and Opportunities, Reference Press, New Delhi [2010], Pg.206.
2. <http://www.legalserviceindia.com/article/l146-Cyber-Crime-And-Law.html>
3. http://shodhganga.inflibnet.ac.in/bitstream/10603/130487/9/09_chapter%204.pdf
4. https://www.researchgate.net/publication/262388740_Latest_Face_of_Cybercrime_and_Its_Prevention_In_India
5. <http://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf>
6. <http://www.ijcrt.org/papers/IJCRT1807078.pdf>
7. <file:///C:/Users/user/Downloads/SSRN-id2486125.pdf>
8. https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Molly_Ghosh.pdf
9. General Assembly resolution 55/25 of 15 November 2000
10. <https://indiankanoon.org/doc/170577355/> retrieved on 02/10/2016
11. <http://www.un.org/womenwatch/daw/cedaw/> retrieved on 02/10/2016.



REJUNIVATING CYBER LAWS TO SHIELD WOMEN FROM CYBER CRIMES

Dr. T. Ambika

*Assistant Professor, School of Law, Sathyabama Institute of Science and Technology
Chennai, Tamil Nadu*

Introduction:

The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Internet makes human beings comfy in their routine life. Information technology has widened itself and has become the main spring of today's global and technical development. In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term 'Cyber' became more familiar to the people. With the numerous advancement of internet, the crime using internet has also widened its roots in all directions. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up which gave birth to cyber crimes at the domestic and international level as well.

With the emergence of technology the misuse of technology has also expanded to its optimum level and then there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect technological advancement system.

CYBER CRIMES

Though the word Crime carries its general meaning as "a legal wrong that can be followed by criminal proceedings which may result into punishment" whereas Cyber Crime may be "unlawful acts wherein the computer is either a tool or target or both"¹

Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes.²

It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include 'denial of services' and viruses attacks preventing regular traffic from reaching your site.

Cyber crimes are not limited to outsiders except in case of viruses and with respect to security related cyber crimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cyber crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual

¹ <https://definitions.uslegal.com/c/cybercrimes/>

² The Information Technology Act, 2000.



property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc. Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cyber crime and what is the conventional crime so to come out of this confusion, cyber crimes can be classified under different categories which are as follows:¹

1. Cyber Crimes against Persons:

There are certain offences which affects the personality of individuals can be defined as:

- **Harassment via E-Mails:** It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails, Facebook, Twitter etc.
- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials.
- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- **Cracking:** It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.

¹ Harpreet Singh Dalla & Ms. Geeta, Cyber Crime – A Threat to Persons, Property, Government and Societies, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X, Available online at: www.ijarcsse.com



- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.¹

2. Crimes Against Persons Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

- **Intellectual Property Crimes:** Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.
- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer.
- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorised person, of the Internet hours paid for by another person. The person

¹ Kharat, Shital, Cyber Crime – A Threat to Persons, Property, Government and Societies (March 1, 2017). Available at SSRN: <https://ssrn.com/abstract=2913438> or <http://dx.doi.org/10.2139/ssrn.2913438>



who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.¹

3. Cybercrimes Against Government:

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.²

4. Cybercrimes Against Society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons.
- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

¹ Dhawesh Pahuja, CYBER CRIMES AND THE LAW, Posted On July 17, 2011 by Legal India, Legal New and Law Resource Portal, <https://www.legalindia.com/cyber-crimes-and-the-law/>

² Opcit., Harpreet Singh Dalla & Ms. Geeta, Cyber Crime – A Threat to Persons, Property, Government and Societies



- Financial Crimes: This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- Forgery: It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.¹

CERTAIN FORMS OF CYBER CRIMES AGAINST WOMEN

There are various types of cyber crimes committed against the women at large, of which some have sensitive effects on the image and security of women are as follows:-²

Cyber Stalking: "Cyber Stalking is the use of the internet or other electronic means to stalk or harass an individual, a group of individuals or an organization. It may include the making of false accusations or statements of the fact, monitoring, making threats, identity theft, damage to data or equipment, and the solicitation of minors for sex, or gathering information that may use to harass."³

It is one of the most talked about cyber crimes which usually occurs with women and children who are stalked by men, adult predators or pedophiles. Oftentimes, the victim of cyber stalker is new on the web and inexperienced with the rules of internet use and safety. There are four reasons behind cyber stalking namely, for sexual harassment, for revenge and hate, for obsession love, and for ego and power trips. Women are targeted via websites, discussion forums, chat rooms, blogs and emails etc. The availability of free emails, and websites space, as well as anonymity has contributed to the increase of cyber stalking as a form of violence.

Cyber Defamation: Cyber violence which includes libel and defamation is another common online crime against women. It occurs when someone posts defamatory matter about someone on website or sends emails containing defamatory information to all that of person's friends. Generally, emotion breakups may lead to the male member to spread lies and false information about the female member to other members through his own posts, community walls, fake profiles etc. The harm through defamatory statements about any person on a website is widespread and irreparable, as the information is available to the entire world, affects the victim as a whole.⁴

Email Spoofing: The common method which is used by men is to email vulgar photographs of themselves to women, praising their beauty and asking for date etc.

¹ Ibid.,

² Halder, Debarati, Cyber crime against women in India, <http://www.cyberlawtimes.com/articles/103.html>

³ Available at; <http://en.wikipedia.org/wiki/Cyberstalking> Accessed on March 11, 2018

⁴ <http://www.helplinlaw.com/employment-criminal-and-labour/CDII/cyber-defamation-inindia.html>, Accessed on March 11, 2018.



In Tamil Nadu, a 21-year-old Salem girl had finished her B.Sc and was looking for a job. The girl found her morphed pictures tagged on her account last week. Upset over the incident, she informed her parents, who registered a complaint with the police on 23 June. However, after the police took on the case, another picture was uploaded on the site along with her father's mobile number, which spurred the girl to commit suicide. The family of the girl have blamed delay in action on the police.¹

According to The Hindu report, the police informed the girl's father that they would need to collaborate with the cyber crime cell to nab the culprits and sought 15 days time for the investigation. However, the girl, after seeing the second image decided to end her life.²

In a separate case October 2015, two boys in Bengaluru along with their friends kidnapped a 15-year-old and clicked her nude pictures. The girl committed suicide. Her suicide note read: "I have decided to die as I have lost my honour. I and my family need justice."³

These are not isolated cases but one of the few cases of online harassment and cyber stalking that were reported by the media. According to National Crime Records Bureau data, the number of cases for obscene publication and transmission in electronic form under the Information Technology Act, 2000, has risen since 2007, when 99 such cases were reported. The number rose to 105 in 2008, 139 in 2009, 328 in 2010, 496 in 2011 and 589 in 2012. The figure more than doubled to 1,203 in 2013. In 2014, 758 crimes were reported, in which 491 people were arrested.

"Online harassment and cyber crimes have not been given the kind of priority in India as these deserve. The mindset is such that these crimes are perceived as minor crimes. And going by the numbers, we know that by and large, India has failed in getting the requisite cyber crime convictions, and the number of such crimes is rising," said cyber law expert and Supreme Court advocate Pavan Duggal.

In an instance, a couple enters in a chat room agreeing to strip for each other using a web camera. The guy stripped, but the person at the other end was actually another man and his friends, who obviously didn't. They recorded it and uploaded the clip on a porno website. These things happen in every city but only one in every 500 cases is reported."⁴

Cyber Pornography is another type of online threat to women's security. It is the graphic, sexually explicit subordination of women through pictures or words that also includes pornography is verbal or pictorial material which represents or describes sexual behavior that is degrading or abusive to one or more of participants in such a way as to endorse the

¹ The Times of India, June 28, 2016.

² The Hindu, June 29, 2016.

³ Deccan Herald, Bengaluru, October 6, 2015.

⁴ Pavan Duggal is one of the pioneers in the field of cyber law. He is practicing Advocate, Supreme Court of India and a cyber law consultant. He is the founder president if Cyber law Asia. Accessed on July 30, 2013, Available at; <http://www.cyberlaws.net/cyberindia/column.htm>



degradation. The person has chosen or consented to be harmed, abused, subjected to coercion does not alter the degrading character of such behavior. Cyber Space has provided medium for the facilitation of crimes like pornography.

Websites show pornographic material on internet today. It can be reproduced more cheaply and quickly on new media like hard disk, floppy disk, and CD-ROMs. Full motion video clips and complete movies are also available now besides still pictures and images. According to IT Amendment Act 2008, crime of pornography under section 67-A, whoever publishes and transmits or causes to be a published and transmitted in the electronic form any material which contains sexually explicit act or conduct can be called as pornography. Section 292/293/294, 500/506 and 509 of Indian Penal Code, 1860 are also applicable.

Cyber Morphing is related with pornography and we can also say it, a cyber obscenity. Female members' photographs are taken from their personal albums and are morphed for pornographic purpose by using parts of the pictures, for example, the head and up to breast. Female pictures are downloaded by fake users and again reposted on different websites by creating fake profiles after morphing them. This is the violation of Information Act 2000, and attracts section 43 and 66 of this act. It can also be booked under Indian Penal Code. Lack of awareness of these types of crimes encourages criminal to commit this mischief.

Cyber Hacking: In this kind of cyber violence, some particular targets are chosen for hacking their profiles, using their personal information for evil purposes. Moreover, the hacker may even distribute open invitations for having sex with the profile owner at her home address. Section 43(a) and 66 under IT amendment Act, 2008 and section 379 and 406 of Indian Penal Code are applicable for punishment after the law regarding cyber hacking is broken.

Virtual Rape via Cyberspace is another violent and brutal type of cyber victimization where women are targeted by the scoundrels or harassers in the cyber space. He either posts vulgar messages such as, "I will rape you", "I will tear you up", "your internet id will be f..ed off" etc, or particular community members may "mob attack" the targeted female with such words which successfully creates more enthusiasm among other unrelated members to comment on the victim's sexuality. Then the profile owner becomes a hot topic vulgar name calling, erotic discussions, sexual image etc.

In the recent past, journalists like Barkha Dutt, student leaders like Shehla Rashid, and actors like Swara Bhaskar have faced horrific online abuse. Rape and death threats and other forms of gendered abuse have been directed at them for merely expressing their opinions online.

A major consequence of online abuse is the silencing effect it has on women, sometimes forcing them to shut themselves out of online spaces. A survey by Feminism in India, a digital platform, found that 28% of women who experienced online abuse said they intentionally reduced their online presence. Amnesty International conducted a study on online



violence against women in 2017 which showed that more than 75% of women surveyed across eight countries (Denmark, Italy, New Zealand, Poland, Spain, Sweden, the UK and USA) who had experienced abuse or harassment made changes to the way they used social media platforms.¹

These are some most discussed forms of cyber victimization against women in cyber space which generally occurs in our super-macho society. Apart from these, cyber victimization encompasses cyber bullying, cheating, phishing, domestic violence via cyber flame, impersonate, blackmailing etc. Unfortunately, Information Technology Act 2000 which was also amended for cyber security in 2008 deals with such offences but it does not mention any crime specifically as against women and children. Thus, it still needs to be modified and strictly to be undertaken.

INFORMATION TECHNOLOGY LEGISLATIONS IN INDIA

The Information Technology Act, 2000

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000. The Act essentially deals with the following issues: Legal Recognition of Electronic Documents, Legal Recognition of Digital Signatures, Offences and Contraventions, Justice Dispensation Systems for cyber crimes.

It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives stated in the preface to the Act, "to provide 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, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The Information Technology Amendment Act 2008

Information Technology Act Amendment which came into force after Presidential assent in Feb 2009 has following salient features:

Liability of body corporate towards Sensitive Personal Data-New amendment was brought in changes in section 43 of IT Act 2000 in which for the first time any body corporate which deals with sensitive personal information does not have adequate controls resulting in wrongful loss or wrongful gain to any person is liable to pay damages to that person to the tune of five crores.

Introduction of virus, manipulating accounts, denial of services etc made punishable-Section 66 has been amended to include offences punishable as per section 43 which has also been amended to include offences as listed above; punishment may lead to imprisonment which may

¹ <https://amnesty.org.in/need-talk-online-violence-women-india-2/>



extend to three years or with fine which may extend to five lakh rupees or with both. This is a change from earlier position where introduction of virus, manipulating some ones account has been made punishable with imprisonment for the first time.

Phishing and Spam- While this has not been mentioned specifically but this can be interpreted in the provisions mentioned here in section 66 A. Through this section sending of menacing, annoying messages and also misleading information about the origin of the message has become punishable with imprisonment up to three years and fine

Stolen Computer resource or communication device – Newly added Section 66B has been introduced to tackle with acts of dishonestly receiving and retaining any stolen computer resource. This has also been made punishable with three years or fine of one lakh rupees or both.

Misuse of Digital Signature-Section 66C. Dishonest use of somebody else's digital signature has been made punishable with imprisonment which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

Cheating-Cheating using computer resource has been made punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee (section 66D)

Cyber terrorism- The newly introduced section 66F talks about acts of cyber terror which threatens the unity, integrity or sovereignty of India or strike terror in the people or any section of the people include

1. Denial of service of resources in use by nation
2. Attempting to penetrate or access a computer resource without authorization or exceeding authorized access

Introducing or causing to introduce any computer contaminant likely to cause death or injuries to person or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or

knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or



otherwise, commits the offence of cyber terrorism. These acts have been made punishable with Imprisonment which may extend to imprisonment for life.

Child Pornography– Newly introduced section 67 B attempts to address the issue of child pornography. Through this section it has made the publication or transmission of material in any electronic form which depicts children engaged in sexually explicit act or conduct, any one who creates, facilitates or records these acts and images punishable with imprisonment of five years and fine which may extend up to ten lakhs in first offence and seven years and fine of ten lakhs on subsequent offence

Intermediary's liability– Intermediaries have been made liable to retain any information in the format that Central government prescribes. (Sections 67C) and are punishable for violation with a punishment of imprisonment of 3 years and fine In case of any act which affects national sovereignty intermediaries are liable to seven years (Section 69(4))

Surveillance, Interception and Monitoring– In order to combat cyber terrorism the government has further armed itself with drastic powers Sections 69 of IT Act 2000 amended enhances the scope from the 2000 version to include interception and monitoring. This has been a major change in the section which also empowers government not only to monitor any traffic but also block any site through any intermediary. Any failure on part of the intermediary is punishable by seven years and also fine (Section 69(4)). Earlier the provision did not mention any fine.

Cognizance of cases– All cases which entail punishment of three years or more have been made cognizable. Offences with three years punishment have also been made bailable (Section 77B). This change though welcome will make sure most cases falling under IT Act will be bailable with sole exception of Cyber terrorism cases, cases related to child pornography and violations by intermediaries in some cases.

Investigation of Offences– One major change has been inclusion of Inspectors as investigating officers for offences defined in this act (section 78). Earlier these investigations were being done only by an officer of the rank of Deputy Superintendent of Police which was a serious limitation mainly because number of officers in this rank is limited. With this change one can look forward to more cases being filed and investigated by police.

SHORTCOMINGS OF THE ACT

Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient.

While the Act has been successful in setting down the frame work of regulations in Cyber Space and addresses a few pressing concerns of misuse of technology, it suffers from a few serious lacunae that have not been discussed. the Act is a toothless legislation, which has



not been completely effective in issuing penalties or sanctions against perpetrators who choose to misuse the reach of cyber space. There are certain areas of cyber laws which need attention¹

Spamming: Spam may be defined as Unsolicited Bulk E-mail. Initially it was viewed as a mere nuisance but now it is posing major economic problems. In the absence of any adequate technical protection, stringent legislation is required to deal with the problem of spam. The Information Technology Act does not discuss the issue of spamming at all. USA and the European Union have enacted anti spam legislation. In fact Australia has very stringent spam laws under which the spammers may be fined up to 1.1 million dollars per day.

Phishing: Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail and often directs users to enter personal and financial details at a website. Phishing is an example of social engineering technique used to fool users. There is no law against phishing in the Information Technology Act though the Indian Penal Code talks about cheating, it is not sufficient to check the activity of phishing. Recently a phishing attack was noticed on the customers of State Bank of India in which a clone of the SBI website was used. What is worse is that even SBI has not alerted its customers. So the need of the hour is a legislation which prohibits the activity of phishing in India.

Data Protection in Internet Banking: Data protection laws primarily aim to safeguard the interest of the individual whose data is handled and processed by others. Internet Banking involves not just the banks and their customers, but numerous third parties too. Information held by banks about their customers, their transactions etc. changes hand several times. It is impossible for the banks to retain information within their own computer networks. High risks are involved in preventing leakage or tampering of data which ask for adequate legal and technical protection. India has no law on data protection leave alone a law governing an area as specific as protection of data in electronic banking.

The Information Technology Act talks about unauthorized access but it does not talk about maintaining integrity of customer transactions. The act does not lay down any duty upon banks to protect the details of customers and clients. U.K has a data protection law which was enacted 10 years back that is in 1998 under which banks or any person holding sensitive information may be held liable for damages if it fails to maintain adequate security protection in respect of data. In India, a bank's liability would arise out of contract as there is no statute on the point.

¹ International cyber security law developments in 2015, Pavan Duggal in Cyber Laws in Today's Times | India | ET <https://blogs.economictimes.indiatimes.com/Cyberlawsintodaystimes/international-cyber-security-law-developments-in-2015/>



Privacy Protection: Privacy and data protection are important issues that need to be addressed today as information technology assumes greater importance in personal, professional and commercial spheres. The European Union and the United States have strict policies relating to privacy and protection of personal data when such data or information is being transferred out of their domain.

It also pertinent to note here, that the absence of a specific privacy law in India has resulted in a loss of substantial foreign investment and other business opportunities. This deficiency has also served as an obstacle to the real growth of electronic commerce. Thus, a statute addressing various issues related to privacy is of utmost importance today, if not an entire act can be brought into force, then at least specific provisions relating to privacy and data protection be incorporated into the Act.

Identity Theft: Identity theft worldwide is a growing problem. IT act 2000 fails to address this issue. This is a major drawback considering the fact that majority of outsourcing work that India does requires the companies in India to ensure there is no identity theft. In fact identity theft was one of the main reasons for a major hue and cry over an incident involving personal information of UK customers and an Indian web marketing company.[vi]

Cyber War: The issue of Cyber War has also not been discussed in the Act. International law is an important part of any legal regime and due provisions need to be made in congruence with the international framework of laws. India, in recent times, has faced a number of cyber attacks from China and the Chinese hackers have overridden the Firewalls on Indian databases like a Mongol army on rampage. In the 26/11 attacks a number of classified data were provided as intel to the perpetrators from neighbouring nations conspiring against India. There are no provisions in the Act to make such perpetrators liable for their actions.

In an interview Mr. Duggal stressed the need for overhauling the cyber security legal regime in the country, saying, "A historical mistake was made when the IT (Amendment) Act, 2008, made almost all cyber crimes, barring a couple, bailable offences. The focus is more on enhancing the quantum of civil liability and reducing the quantum of punishment, which explains the reason why the number of cyber crime convictions in the country is in single digits."

Even the Internet Service Providers (ISP) who transmits some third party information without human intervention is not made liable under the Information Technology Act, 2000. One can easily take shelter under the exemption clause, if he proves that it was committed without his knowledge or he exercised due diligence to prevent the offence. It's hard to prove the commission of offence as the terms "due diligence" and "lack of knowledge" have not been defined anywhere in the Act. And unfortunately the Act doesn't mention how the extra territoriality would be enforced. This aspect is completely ignored by the Act, where it had



come into existence to look into cyber crime which is on the face of it an international problem with no territorial boundaries.

SUGGESTIONS FOR IMPROVEMENT

- The IT (Amendment) Act, 2008, reduced the quantum of punishment for a majority of cyber crimes. This needs to be rectified.
- The majority of cyber crimes need to be made non-bailable offences.
- The IT Act does not cover a majority of crimes committed through mobiles. This needs to be rectified.
- A comprehensive data protection regime needs to be incorporated in the law to make it more effective.
- Detailed legal regime needed to protect privacy of individuals and institutions.
- Cyber war as an offence needs to be covered under the IT Act.
- Parts of Section 66A of the IT Act are beyond the reasonable restrictions on freedom of speech and expression under the Constitution of India. These need to be removed to make the provisions legally sustainable.

CONCLUSION

The Information Technology (Amendment) Act, 2008 serves as for an analysis of the legislative exercise of law and policy formulation in the field of cyber crime legislation. This study reveals that quite emphatically the need for carefully worded provisions, foresight in the drafting process and imagination with respect to explanations to particular sections. The inadequacies of the legislation and the resultant realistically anticipated problems reinforce the notion that criminal legislations cannot be left open to broad interpretations, especially with regard to internet regulations, considering the fact that cyberspace provides certain liberties in action that make it easier to transgress laws, and with such characteristics inherent to the environment, any regulatory mechanism or legislative measure must seek to be comprehensive, clear and narrow in interpretive scope.

While the purpose of the Information Technology (Amendment) Act was to address increasing trends of cyber crime, in actual practice, make it difficult to identify a cyber criminal, the irony rests in the fact that what the Amendment Act eventually has created is a situation wherein it perhaps, isn't 'easier to be a criminal', but rather, 'easier to be classified as a criminal'. The danger, in both cases, cannot be overemphasised.

§The existing laws fall short to tackle the situation. India must bring in more rigid and stringent laws in protecting women from cybercrime. The menace of cybercrime is not just restricted to India, but to the whole of world. Hence, there is a need for coordinated and integrated effort on part of the world community. Proper implementation of laws along with public awareness and education of women concerning their rights and legal remedies will play a crucial role in eradicating cybercrimes from our society.



THE SOCIAL IMPACT OF PHISHING ATTACK- AN ANALYSIS

Mr. Mohamed Salihu M.,

Assistant professor in Sociology,

School of Law, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu.

INTRODUCTION

The word "phishing" comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users. The term phishing was coined in the 1996 timeframe by cybercriminals who were stealing America On-Line accounts by scamming passwords from unsuspecting AOL users. The first report on the Internet phishing is on the alt.2600 hacker newsgroup in January 1996; however the word may have been used even earlier in the printed edition of the scammer newsletter "2600". "Ph" is a common scammer replacement for "f", and is a nod to the original form of hacking, known as "phreaking". Phreaking was coined by the earliest hacker, John Draper. John invented "hacking" by creating the infamous Blue Box, a tool that he used to hack telephone systems in the early 1970s. This first form of hacking was known as "Phone Phreaking".

The blue box emitted tones that allowed a user to restrain the phone switches, thereby making long distance calls for free, or billing calls to someone else's phone number. This is in fact the origin of a lot of the "ph" spelling in many hacker pseudonyms and scammer organizations. By 1996, hacked accounts were called "phish", and by 1997 phish were actually being traded between cybercriminals as a form of currency. People would routinely trade 10 working AOL (America On-Line) phish for a piece of hacking software that they needed. Over the years, phishing scams grew from simply stealing AOL (America On-Line) dialup accounts into a more sinister criminal enterprise. Phishing scam now target users of online banking, payment services such as Paytm, PayPal, and online e-commerce sites. Phishing attacks are growing rapidly in number and sophistication.

Phishing attacks in India

According to the RSA Quarterly Fraud Report for the period between January 1 to March 31, 2018, phishing accounted for 48 per cent of all cyber-attacks. The report that contains cyber fraud attack and consumer fraud data and analysis, noted that Canada, the United States, India and Brazil were the countries uttermost targeted by phishing. Other uttermost phishing-targeted countries include Brazil in the fourth place, Netherlands (5th), Colombia (6th), Spain (7th), Mexico (8th), Germany (9th) and South Africa (10th). As per the report, consumer transactions and cyberfraud continue to grow in the smartphone channel. In the first quarter, 55 per cent of transactions originated in the smartphone channel and 65 per cent of fraud transactions used a mobile application or browser.

The report further noted that the top hosting countries list for such attacks was topped by the United States, followed by Russia and India in the second and third place, respectively. Others in



the list comprise Australia in the fourth position, Canada (5th), France (6th), Luxembourg (7th), Germany (8th), China (9th) and Italy (10th). The report represents a snapshot of the cyber scam environment, providing actionable intelligence to consumer-facing organizations of all sizes and types to enable more effective digital risk management.

In the year 2017, CERT-In (Indian Computer Emergency Response Team) handled 53081 incidents. The types of incidents handled were, Malicious Code, Phishing, Distributed Denial of Service scams, Website intrusion & Malware propagation, Website Defacements and pirated Scanning activities. In addition, 53692 spam incidents were also reported to CERT-In. The summary of various types of incidents handled is given below:

Table 1: Breakup of Security Incidents handled various types of incidents handled by CERT-In

Security Incidents	2017
Phishing	552
Network Scanning / Probing	9383
Virus/ Malicious Code	9750
Website Defacements	29518
Website Intrusion & Malware Propagation	563
Others	3315
Total	53081

REVIEW OF LITERATURE

The researcher evaluated books, journals, newspapers and Govt. reports to summarize the literature review and followings are the review of literature for this study:

Paul T. Augastine (2007) Phishing is a rapidly growing threat in cyber world and causing billions of dollars in damage each and every year to internet users. It is an illegal activity which uses a group of social engineering and technology to collect an Internet user's sensitive information. The identification of phishing techniques can be performed in diverse methods of communications like email, pop-up messages, instant messages or at web page level. Over the period, many research articles have published with different techniques and procedures but have failed to detect all associated risks and provide a comprehensive solution.

Majid yar(2006) Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a reliable entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate site.

G.Ram Kumar (2006) Phishing is the internet age crime, born out of the technological advances in internet age. "Phishing" is a newer form of social engineering. Typically, Phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensible information, such as passwords, usernames, login IDs, ATM PINs and credit card details, by masquerading as a



trustworthy person in an apparently official electronic communication, such as an email or an instant message.

Anjali Kaushik (2013) Due to the broad nature of the phishing problem, he find important to visualize the life-cycle of the phishing scams, and based on that categorize anti-phishing solutions. He depict a flowchart describing the life-cycle of phishing campaigns from the perspective of anti-phishing techniques, which is intended to be the most comprehensive phishing solutions flowchart.

Dr.M.Dasgupta (2009)Phishing is an act of attempting a victim for fraudulently acquires sensible information by impersonating a trustworthy third party, which could be a person or a reputed business in an electronic communication. The objective of phishing attack is to trick receivers into divulging sensitive information such as bank account numbers, passwords and credit card details. For instance, a phisher may misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the receiver.

Julie S. Downs(2007)He surveyed 232 computer users to study what are the criteria that can predict the susceptibility of a user to fall victims for phishing emails. The survey was formed in a role play where each user was anticipated to analyze emails as well as answering a number of questions. The outcome of the study was that those who had a good knowledge about the definition of “phishing” were significantly less likely to fall for phishing emails, while knowledge about other areas, such as spyware, cookies and viruses did not help in reducing vulnerability to phishing emails. Interestingly, the survey showed that knowledge about negative consequences (e.g. credit card theft) did not help in reducing vulnerability to phishing emails and web pages. The study concluded that user educational messages should focus on educating users about phishing scams rather than warning them about the dangers of negative consequences

Huajun Huang (2009) the primary reasons that lead technology users to fall as victims for phishing attacks are:

- Users ignore passive warnings (e.g. toolbar indicators).
- A large number of users cannot distinguish between phishing and legitimate sites, even if they are told that their ability is being tested.

Steve Shen (2013)He shows a number of indirect characteristics that correlate between victims and their susceptibility to phishing scams. According to his study, age and gender strongly correlate with phishing susceptibility. They conclude that:

- Females tend to click on email links more often than males.
- People between 18 and 25 years old were much more likely to fall victim to phishing scams than other age groups. This was justified to be caused by a lack of sufficient experience and technical knowledge.



RESEARCH METHODOLOGY

Statement of the problem

“We've seen a sharp decrease in phishing site activity since deploying the Tipping Point anti-phishing filters, and block more than 9,000 phishing attacks per hour.”- Randy Williams.

The problem with phishing is that attackers constantly look for new and creative ways to fool users into believing their actions involve a legitimate website or email. Phishers have become more skilled at forging websites to appear identical to the expected location, even including logos and graphics in the phishing emails to make them more convincing.

There are dangerous new advanced phishing methods that utilise personal information that is easily available to the public in order to produce plausible and believable attacks that directly target victims. Methods such as social phishing and context aware phishing are perfect examples of attacks utilising the massive amount of public information to increase the effectiveness of their scams.

Statistics (All over the World):

- 156 million phishing emails sent everyday
- 16 million phishing emails make it through filters
- 8 million phishing emails are opened
- 800,000 links are clicked from the phishing emails
- 80,000 people fall for the scam every day, and give away personal information to people who are trying to phish them.
- 9% of online Canadians have replied to spam mail unknowingly
- 7% have replied to spoof or phishing mail unknowingly
- 3% have entered bank details on a site they don't know, that's over 1 million Canadians in total
- 95 percent of phishing e-mails pretend to be from Amazon, eBay, or banks.

Objectives

The followings are the objectives of this research paper

- To analyse the various types of Phishing.
- To describe the social impact of phishing.
- To identify the range of techniques in use phishing.
- To examine the causes of criminal behaviour of the phishers by applying social control theory.
- To evaluate the solutions for phishing.

Research design

The Researcher used descriptive research method to analyze the secondary data which is about social impact of phishing attack and its solutions.

TYPES OF PHISHING



Phishing is an act that attempts to electronically obtain delicate or confidential information from users (usually for the purpose of theft) by creating a replica website of a legitimate organization. Phishing is usually perpetrated with the aid of an electronic device/tools (and a computer network; they target the weaknesses existing in various detection systems caused by end-users (who are considered to be the weakest element in the security sequence).

There are different types of phishing attacks prevalent at present scenario. The researcher categorizing the phishing attack into different kinds:

Email Phishing

Phishing scam on the Internet starts with an email message that looks like an official communication from a reliable source such as a bank, a credit card company or a reputable online store. In the e mail recipients, are directed to a fraudulent website where they are asked to provide personal information such as account numbers and/ or passwords. Message is sent out to several people where they for example are told that there are problems with some credit from the bank. The problem, however, according to e-mail, easily solved by following an attached link to a website, where the victim is asked to enter his personal data like name, DOB and credit card details. This data are then used to tap money from the card. It is all made more credible when the e-mail looks like it is from a reputable bank and that the website you come to look quite like the official website of this bank, defraud clean using a script that first open the bank's actual website and then a smaller window, which loads from the attacker's server, where the address bar is not visible. This allows for many looks as you come into the bank's website, and it feels safer to enter the appropriate information. Figure 1 shows the email phishers web page that will help us to understand what email phishing is.



Figure: 1

Ransomware

It is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed information is decrypted and



access returned to the victim. The motive for ransom ware scam is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in a virtual currency, such as bit coin, so that the cyber attacker's identity isn't known. Ransomware malware can be diffuse through malicious email attachments, infected software apps, infected external storage devices and compromised websites. A growing number of cyber-attacks have used remote desktop protocol and other approaches that don't rely on any form of user interaction. In a lock screen variant of a ransom ware scam, the malware may change the victim's login credentials for a computing device; in a data kidnapping attack, the malware may encrypt files on the infected device, as well as other connected network tools. While early instances of these scams sometimes merely "locked" access to the web browser or to the Windows desktop and did so in ways that often could be fairly easily reverse engineered and reopened cyber hackers have since created versions of ransomware that use strong, public-key encryption to deny access to documents on the computer.

Famous ransomware: CryptoLocker and WannaCry

Perhaps the first example of a widely spread attack that used public-key encryption was Crypto locker, a Trojan horse that was active on the internet/ web pages from September 2013 through May of the following year. The malware urged payment in either bitcoin or a prepaid voucher, and experts generally believed that the RSA cryptography used when properly implemented was essentially impenetrable. In May 2014, however, a security firm gained access to a command-and-control server used by the scam and recovered the encryption keys used in the attacks. An online tool that allowed free key recovery was used to effectively defang the scam.

In May 2017, an attack called WannaCry was able to infect and encrypt more than a quarter million systems globally. The malware uses asymmetric encryption so that the victim cannot reasonably be expected to recover the key needed to decrypt the ransomed documents.

Rock phishing attacks

It is both a phishing toolkit and the entity that publishes the toolkit. Phishing is an email criminal method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. While the authors of the kit remain anonymous, it has become the most popular phishing kit available online, with some estimates suggesting that the kit is used for half of all phishing attack. Rock Phish is known for pioneering the use of image spam. The Rock Phish toolkit first surfaced in the hacking society in 2004. It has also proven particularly adept at evading the adaptive security measures taken by website/networking professionals, earning the group grudging respect for their ability to stay on the cutting point of technology and out of the hands of law enforcement. In beginning of the 21st century, a group of phishers arose who were suspected to be working in Eastern Europe.



They were given the name “Rock phish gang” because the early version of their scams contained word “Rock” in the URL. *For example:*

‘<http://www.bankname.securesite.com/rock/234/signing.html>’

They are still very active although they are not using the same naming convention. They have targeted multinational and local banks throughout USA, Europe and South America.

Man – in – The - Middle Phishing attack

Man in the middle Phishing attack(MITM) is an attack where the attacker secretly relays and possibly alters the communication between two individuals who believe they are directly communicating with each other. One example of a MITM is active eavesdropping, in which the scammer makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection/network, when in fact the entire conversation is controlled by the hacker. The scammer must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted wireless access point could insert himself as a man-in-the-middle. Figure 2 shows the functions of MITM that will help us to understand what Man in the middle Phishing attackis.

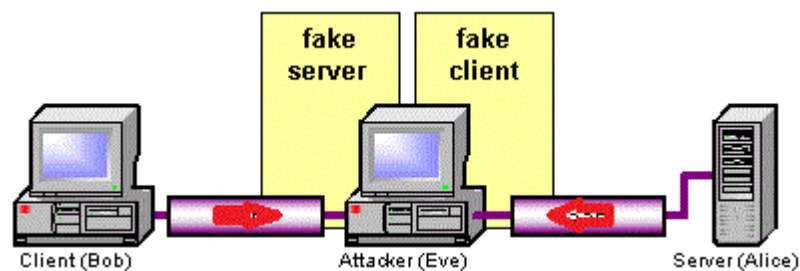


Figure:2

Example of MITM

Session Hijacking

Session hijacking is taking over a user session. Essentially it is when two computers establish a connection and a scammer assumes the position of one of the computers through their session id. Session hijacking can be performed locally on a user’s computer, or remotely as a part of a man-in-the-middle attack. This form of attack is performed on two levels. Session hijack attacks on the application layer are performed through TCP and UDP while hijacking on the network layer involves the hijack of HTTP sessions.

These two kinds of attacks can often occur simultaneously, but it depends on the system being attacked. Attacks on network level are most appealing for the attacker. The reason for this being that their attacking program does not have to be tailor-made for the web application. It simply can attack the data flow of the protocol, and that is common for all web applications.



Types of session hijacking

Session fixation, where the attacker sets a user's session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs

Cross-site scripting, where the attacker tricks the user's computer into running code which is treated as trustworthy because it appears to belong to the server, allowing the scammer to obtain a copy of the cookie or perform other operations.

Session side jacking, where the scammer uses packet sniffing to read network traffic between two parties to steal the session cookie.

Many web sites use SSL encryption for login pages to prevent scammers from seeing the password, but do not use encryption for the rest of the site once authenticated. This allows scammers that can read the network traffic to intercept all the data that is submitted to the server or web pages viewed by the client. Since this information includes the session cookie, it allows him to impersonate the victim, even if the password itself is not compromised. Figure 3 shows the functions of Session hijacking which will help us to understand what Session hijacking is.

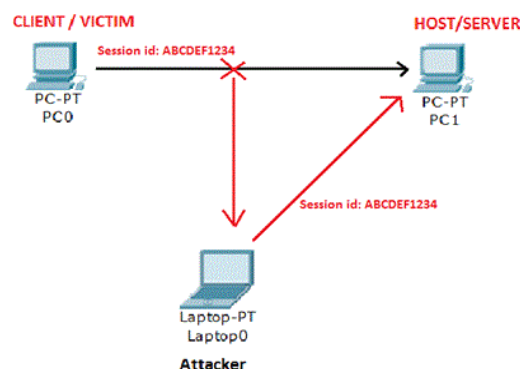


Figure:3

Content Injection phishing:

Content injection phishing is a kind of phishing in which the attacker put in harmful content into a normal legal website. The content has is able to redirect the user to other sites and install malware on users machine. It can also insert a frame of content which redirect data to a phishing server. Figure 4 shows the scammer web page that will help us to understand what Content injection phishing is.

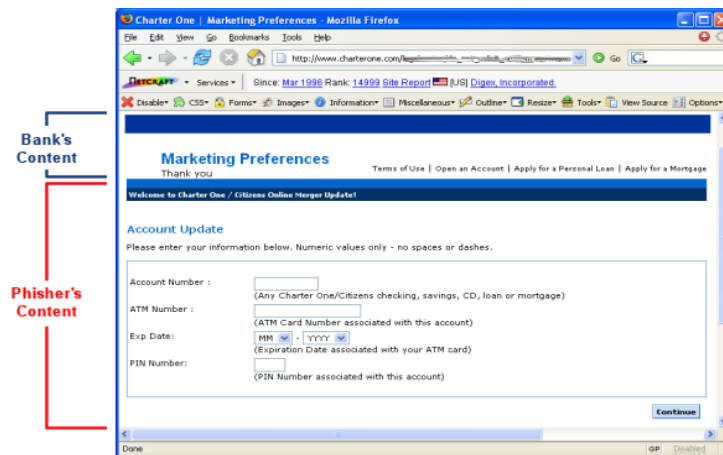


Figure:4

Search Engine Phishing

Another injection method that phishers use to lure users is that they make fake web pages for products and services; search engines find these pages and give them index, so that in a search done by a user, the search engine offers fake pages as elements of search result.

These pages offer usually goods and services in a very reasonable price. For example, a phisher creates a page advertising an interest rate slightly higher any other real banks. Tempted victims who have found these pages via search engines, enter their bank account credentials for a “balance transfer” to the “new account”. The phisher receives sensitive information as part of an order, sign-up or balance transfer. Figure 5 shows that the search engine phisher web page that will help us to understand what search engine phishing is.



Figure:5

SOCIAL IMPACT OF PHISING

The impact of phishing is far more insidious than just an invasion of privacy. It is used to compromise computer security through social engineering. It can be used to steal money, steal data, disrupt computer operations, ruin reputations, destroy important information or feed the ego of an attacker. So when it comes to the people and society, phishing attacks are really damaging the internet. we can always find some scams in your junk mail folder or ads on the Facebook and twitter that try to link you to a fake website. With the fast growing phishing



technology and rising social networking, people are getting more risks when they are sharing the personal data in online. For instance, China has the most internet users in the world, there're about 200 million of them use online shopping and/or online business. Online shopping has become very popular, because all user needs is a computer that is connected to the internet or even a smartphone. But it has been officially reported that there are 10 thousand phishing websites been created every day, 95% of them are auto-generated by scammers computers themselves. Traditional anti-phishing technologies are lacking of identifying those networks/websites. Most people that use online shopping have encountered the phishing scams or similar traps, 80% of the phishing websites are getting viewed by both buyers and sellers and 20% of the phishing are succeed. The methods used by spammers have become more sophisticated, and spam is now increasingly combined with malware and used as a device for online scam or theft.

The damage caused by phishing scam does not only apply to monetary property alone. The fragile bonds of trust that company build with their constituents are shattered in the process. As people loss reliance in the reliability of electronic communication methods, companies loss their customer base. In the case disasters, people can spend billions in preparation, to analyze weaknesses and improve recovery time, only to have thrust shattered by phishing scams. This in turn causes a significant loss in time, money and resources.

SOCIAL CONTROL THEORY

This theory describes internal means of social control. It has become one of the more widely accepted explanations in the field of criminology in its attempt to account for rates in crime and deviant behaviour. Unlike theories that seek to explain why people engage in deviant behaviour, social control theories approach deviancy from a different direction. The theory seeks to explain how normative system of rules and obligations in a given society serve to maintain a strong sense of social cohesion, order and conformity to widely accepted and established norms.

Social control theory was developed by American Sociologist Travis Hirschi in 1969. He refers to four elements which constitute the societal bond. The followings are the important social bonds to maintain a strong sense of social cohesion, order and conformity to widely accepted and established norms.

- 1) Attachment – to the other individuals
- 2) Commitment – to following rules
- 3) Involvement –to typical social behaviors
- 4) Belief – a basic value system.



Theoretical frame work

Attachment	Commitment
Social Bond/Social control	Involvement Belief

Figure:6

Figure 6 shows that the theoretical framework of social control theory that will help us to understand the causes of criminal behaviour of phishers. Attachment, Commitment, Involvement and Belief are the important elements for the social bond/ social control of the individuals in the society. When one of these four elements break down, Hirschi hypothesizes that an individual may participate in criminal activities.

CONCLUSION AND SOLUTIONS

Phishing is an vital problem that results in identity theft. Although simple, phishing attacks are sorely effective and have caused billions of dollars of damage in the last couple of years. In many cases, the phisher does not directly cause the economic damage, but resells the illicitly obtained data on a secondary market. Hence, phishing scams are still and important problem and solutions are required. Phishers use the downloaded webpage from the real Web site to make the phishing webpage appears entirely the same as the real one does. Actually, phishing webpage detection is similar to duplicated or plagiarized document detection in some extent. Digital watermarking is one of the most widely used appraisals to protect digital information from copyright infringements. Detecting the phishing websites is one of the crucial problems facing the internet community because of its high impact on the daily online transactions performed.

Phishing preys upon the susceptibility of the end user to divulge sensitive to a seemingly trustworthy source. This makes it exceptionally difficult to combat at a user level because to attempt to create an educated user base across the entirety of the internet seems a difficult, if not impossible task. A large number of the anti-phishing techniques currently employed experience a lag period between correctly identifying and blocked phishing campaigns, however there have been promising strides taken forward in recent developments with email and content filters as well as heuristics surrounding identification of phishing attacks.

In this paper, researcher observed the social impact of phishing and the followings are the Solutions. But absolute security from phishing is myth.

Keep Informed About Phishing Techniques

New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, we could inadvertently fall prey to one. Keep eyes peeled for news about new phishing scams. By finding out about them as early as possible, we will be at much lower risk of getting snared by one. For IT administrators, ongoing security awareness training and simulated phishing for all users is highly recommended in keeping security top of mind throughout the company.



Think Before Click

It's fine to click on links when we're on trusted sites. Clicking on links that appear in instant messages and random emails, however, isn't such a intelligent move. Hover over links that we are unsure of before clicking on them. A phishing email may claim to be from a legitimate organization and when you click the link to the website, it may look exactly like the real website. The email may ask to fill in the information but the email may not contain our name. Most of the phishing emails will start with "Dear Customer" so we should be alert when you come across these emails. When we have doubt, go directly to the source rather than clicking a potentially dangerous link.

Install an Anti-Phishing Toolbar

Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing web sites. If we stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing attacks, and it is completely free.

Verify a Site's Security

It's natural to be a little wary about supplying sensitive personal/financial information online. As long as you are on a secure website, however, we shouldn't run into any trouble. Before submitting any data, make sure the site's URL begins with "https" and there should be a closed lock icon near the address bar. Check for the site's security certificate as well. If we get a message stating a certain website may contain malicious files, do not open the website. Never download files from suspicious emails or websites. Even search engines may show certain links which may lead users to a phishers webpage which offers low cost products. If the user makes purchases at such a website, the credit card details will be accessed by phishers.

Check Your Online Accounts Regularly

If we don't visit an online account for a while, someone could be having a field day with it. Even if we don't technically need to, check in with each of our online accounts on a regular basis. Get into the habit of changing our passwords regularly too. To prevent bank phishing and credit card phishing scams, we should personally check our statements regularly. Get monthly statements for financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without our knowledge.

Keep Browser Up to Date

Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers unavoidably discover and exploit. If we typically ignore messages about updating browsers and stop. The minute an update will be available, download and install it.



Use Firewalls

High-quality firewalls act as buffers between user, user's computer and outside intruders. We should use two different kinds: a desktop firewall and a network firewall. The first option is a type of software, and the second option is a type of hardware tools. When used together, they drastically reduce the odds of hackers and phishers infiltrating the computer or network.

Wary of Pop-Ups

Pop-up windows often masquerade as legitimate components of a website/webpage. All too often, though, they are phishing attempts. Many popular browsers allow us to block pop-ups; you can allow them on a case-by-case basis. If one manages to slip through the cracks, don't click on the "cancel" button; such buttons often lead to phishing web sites. Instead, click the small "x" in the upper corner of the screen's window.

Never Give Out Personal Information

As a general rule, we should never share personal or financially sensitive information over the Internet. This rule spans all the way back to the days of America Online network, when users had to be warned constantly due to the success of early phishing attacks. When in doubt, go visit the main website of the company in question, get their number and give them a call get related information. Most phishing emails will direct our web pages where entries for financial or personal information are required. An Internet user should never make confidential entries through the links provided in the emails. Never send an email with sensitive information to anyone. Make it a habit to check the address of the website. A secure website always starts with "https".

Use Antivirus Software

There are plenty of reasons to use antivirus software. Special signatures that are included with antivirus software guard against known technology workarounds, tools and loopholes. Just be sure to keep our software up to date. New definitions are added all the time because new attacks are also being dreamed up all the time. Anti-spyware and firewall settings should be used to prevent phishing scams and users should update the programs regularly. Firewall protection prevents access to malicious documents by blocking the scams. Antivirus software scans every file which comes through the Internet to our computer. It helps to prevent damage to your system.



**CYBER MARKET AND CONSUMER PROTECTION IN CYBER SPACE- AN INDIAN
 SCENARIO**

Dr. M. Maya,

*Assistant Professor, School of Management Studies, Sathyabama Institute of Science and
 Technology, Chennai, Tamil Nadu.*

&

Dr. S. Nithya

*Assistant Professor, School of Management Studies, Sathyabama Institute of Science and
 Technology, Chennai, Tamil Nadu.*

1. INTRODUCTION:

“Electronic commerce means the supply of goods or services or both, including digital products over digital or electronic network”, Section 2(44), The Central Goods and Services Tax Act, 2017, Govt. of India.

E-commerce has been defined differently by various organisations. “E-commerce is understood to mean the production, distribution, marketing and sale or delivery of goods and services by electronic means,” according to WTO Work Programme on E-commerce (1998).

Figure 1: E-Commerce Forms and Transactions

	Government	Business	Consumer
Government	G2G <i>e.g. co-ordination</i>	G2B <i>e.g. information</i>	G2C <i>e.g. information</i>
Business	B2G <i>e.g. procurement</i>	B2B <i>e.g. trade</i>	B2C <i>e.g. trade</i>
Consumer	C2G <i>e.g. tax compliance</i>	C2B <i>e.g. price comparison</i>	C2C <i>e.g. auction market</i>

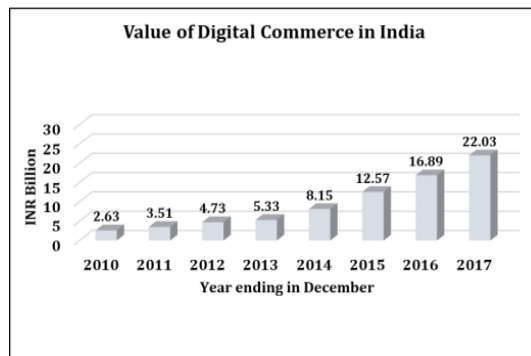
Source: Coppel (2000)⁴

2. E-COMMERCE SECTOR IN INDIA:

“The e-commerce market in India has grown at a compound annual growth rate (CAGR) of 30 per cent between December 2011 and December 2016. It is estimated to reach INR 220,330 crore by December 2017”, Digital Commerce Report 2016. In 2016, 56.37 per cent e-commerce market was covered by travel sector while remaining 43.63 was covered by non- travel sectors, such as e-tail (35.45 per cent), utility services (3.72 per cent), matrimony and classified (2 per cent) and other online services (2.45 per cent).

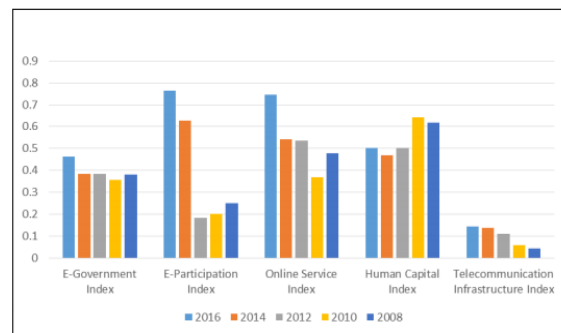


Figure 2: Growth of E-commerce in India



Source: Digital Commerce Report 2016

Figure 3: E-sector Index in India



Source: UN E-Government Knowledge Database

3. CHALLENGES:

Whilst there is political goodwill to foster e-commerce in India, there are still imminent challenges impinging upon its development, such as rural penetrability, taxation, standardisation, cyber-security, data protection, entrenchment of SME, competition regulation, consumer protection and welfare and minimal incentives. Additionally, there is a gap in regulations and/or policy and institutions, despite India has more liberalised e-commerce sector as compared to other regions.

The following are the key challenges for deepening e-commerce between any two regions:

- Difficulties in deciding and collecting custom duties,
- Absence of proper regulatory framework for governing cross-border e-commerce and dispute resolution,
- High rate of cyber risk, frauds and security, for example, risk related to payment and low penetration of debit and credit cards,
- Difficulty in tax and regulatory compliance complemented with ambiguity on applicable tax rates,
- Content restriction on national security and other public policy grounds, which may affect business in the field of information services, such as the media and entertainment sectors,
- Change in product pricing with the change in country/region,
- Complexities in return and exchanges, logistics and reverse logistics,
- Inadequate knowledge and awareness among the buyers/consumers,
- Unreliable transit duration and lack of transparency on delivery, and
- Competition concerns in the big data and artificial intelligence era, particularly the winner-take-all phenomenon.

3.1. Consumers' problems in e-commerce

- **Data security:** A consumer has to share his/her name, contact number, address, bank details and other related information while purchasing goods or services through e-platforms. The data is always at risk of falling in the wrong hands.



- **Digital payments failure:** The refund of online payments generally takes about 5-15 days if the payment process fails and the amount is deducted.
- **Manufacturing and expiry dates not known to the consumer:** While buying offline a customer can always check the best before or the expiry date of the product, but in case of online purchase, the consumer does not know such details. However, the government has recently made it compulsory to show details on e-shopping portals.
- **Delay/fraud in delivery of the goods:** The goods, purchased online, are sometimes not delivered within the timeframe given to the customer. Additionally, either many a times consumers are delivered stone/waste etc. instead of the good or products falling short of quality/size/weight etc. as compared to described on online shopping portal.
- **Origin of the goods is unknown:** Sometimes consumers have to compromise with quality of the product, as the information regarding place of origin of the goods is not displayed at e-shopping platforms.
- **Quality issues:** Many cases have been reported where consumers have received counterfeit or replica goods instead of the original one.
- **Return and refund policies are not clear:** Due to the virtue of e-shopping, a customer can not touch or try the product before purchase. For this companies offer provisions to exchange or return the commodity but sometimes these policies are not clear.
- **Dispute redressal mechanism, especially in case of cross-border exchange:** Dispute redressal is a big challenge from the consumers' point of view as many consumers face several ambiguities between placing an order and receiving the final delivery. This issue becomes complex in case of cross-border exchange.

4. CONSUMER AWARENESS, PROTECTION, AND WELFARE

4.1. UNCITRAL MODEL LAW

United Nations General Assembly adopted the United Nations Commission on International Trade Law (UNCITRAL) model on e-commerce on January 30, 1997, through a resolution.⁸ The UNCITRAL was used as a forum by the government to develop the universally acceptable e-commerce laws. The purpose behind drafting UNCITRAL model on e-commerce was to serve as a base document for creating a uniform international law, which could be used by various countries while amending their own laws and practices on e-commerce. The Information Technology Act, 2000 that facilitates e-commerce and its governance in India, is based on the UNCITRAL model on e-commerce. The Act legally recognises electronic contents, electronic records and electronic transactions.



4.2. E-CONSUMER PROTECTION BY ORGANISATIONS

The OECD, International Chamber of Commerce (ICC), and International Consumer Protection and Enforcement Network (ICEPEAN) are among such organisations, which have issued specific guidelines to protect consumer rights in e-commerce. Moreover, OECD has given some guidelines to protect consumers in online marketplace. Some of the guidelines are as follows:

- Equal consumer protection when buying online or offline
- Disclosure of complete information to the e- consumer, which also includes the information about the transactions
- The payment system must be secure and reliable
- Alternate dispute resolution in the case of international trade

The International Chamber of Commerce (ICC) released 'Guidelines on advertising and marketing on the Internet' in 1996. The guidelines issued by the ICC were meant to set standards of ethical conduct to all promotional activities like marketing and advertising on the internet with respect to consumer protection, such as meeting consumer privacy expectations, to improve public confidence in advertising, minimise the need of governmental legislation etc.

The ICEPEAN aims to preserve and protect the interest of consumers all over the world. It shares information about activities taking place across borders, which might be of use to consumers and promote their interests.

4.3. THE INDIAN LAWS AND E-COMMERCE

India has witnessed a rapid growth in e-commerce, which has resulted in number of cases against consumer rights and welfare also. There are various existing laws, which cover e-commerce in one or the other way. Some of the important such laws are:

- The Foreign Direct Investment (FDI) policy regulates foreign investment into the e-commerce industry,
- Copyright Act 1957 and Trademark Act 1999: If a seller is selling fake goods of a well-known brand through an e-platform, the lawful brand of such goods might sue seller under the said Acts,
- Consumer Protection Act, 1986 (COPRA): COPRA was enacted to protect the rights of consumers. The Act provides six basic rights to the consumers viz., right to be protected against unfair trade practices, right to be informed, right to be assured, right to be heard, right to seek redressal against unfair trade practice and restrictive trade practices and right to consumer education. The consumer has same rights if purchasing goods or services through e-platforms also. The law document covers businesses as customers,
- The Information Technology Act, 2000 (IT Act): The IT Act validates the electronic



transactions stating: “An e-commerce transaction is legal if the offer and acceptance are made through a reasonable mode”. The Act provides legal framework to internet governance and it also gives recognition to digital signatures and electronic records,

- Food Safety and Standards Act, 2006 and Drugs and Cosmetics Act 1940: The e-commerce portal can be penalised under the said Acts for selling adulterated or prohibited goods,
- The Information Technology (Amended) Act 2008: To increase the security of e-commerce transactions, the Act was amended in 2008. The amended Act provides for protecting personal data under Section 43A,
- The Information Technology (Intermediaries Guidelines) Rules, 2011 state that the intermediary must not knowingly host or publish any prohibited information and if done, should remove them within 36 hours of its knowledge, and
- The Consumer Protection Bill, 2018 has only tabled in Lok Sabha and has to go through several processes. It intends to replace the 31- year old Consumer Protection Act 1986 and it will cover e-commerce separately.

5. CONCLUSION

The strong contributory factor is India's political goodwill evidenced through the formulation of its Science Technology and Innovation Policy (STI, 2013), which creates an enabling environment for innovations, such as digital payments, hyper-local logistics, analytics driven customer engagement and digital advertisement. The policy has brought forth a number of promising government initiatives like 'Digital India', 'Start-up India' and 'Make in India' which have begun significantly contributing to the growth of the e-commerce.

References:

- Sanjay Kumar Mangla, Jill Atieno Juma, Ujjwal Kumar, and Jeetali Agnani, “E-Commerce in the Context of Trade, Competition and Consumer Protection in India”, Discussion Paper, www.cuts-international.org
- AMI Perspectiva's (2017). The strongest e- commerce markets in Latin America. (2017, June 30). Retrieved from <http://amiperspectiva.americasmi.com/the-strongest-e-commerce-markets-in-latin-america/> on 09 August 2017.
- ASSOCHAM-Forrester Study India's e-tailing growing fastest in the world. (2016, May 08). Retrieved from <http://www.assochem.org/newsdetail.php?id=5669> on 09 August 2017.
- Asthana, S. (2016, March 30). 100% FDI in online retail: What does it mean for you and the retailers? Business Standard. Retrieved from http://www.business-standard.com/article/economy-policy/100-fdi-in-online-retail-what-does-it-mean-for-you-and-the-retailers-116033000354_1.html on 10 August 2017.
- Desai, R. D. (2015, June 25). A new era for India-Latin America Relations? Forbes. Retrieved from <https://www.forbes.com/sites/ronakdesai/2015/06/25/a-new-era-for-india-latin-america/>



america- relations/#3413d08010e2 on 09 August 2017.

- Ecommerce Foundation. (2014). Latin America B2C E-commerce Report 2014. Amsterdam: Author.
- Ecommerce Foundation. (2015). Global B2C E-commerce Report 2015. Amsterdam: Author.
- Kaplan, M. (2015, February 26). Ecommerce in Latin America: Challenges, opportunities. PracticalEcommerce. Retrieved from <http://www.practicalecommerce.com/Ecommerce-in-Latin-America-Challenges-Opportunities> on 10 August 2017.

REFERENCE

- ❖ James Graham, Cyber fraud: Tactics, Techniques and procedures 27,44-52(2009)
- ❖ Samuel C. McQuade, Understanding and Managing Cybercrime 155-56(2006)
- ❖ Robert W.Taylor, Digital Crime and Digital Terrorism 3 (2006)
- ❖ Dr.M.Dasgupta, Cyber Crime in India: A Comparative Study 53(2009)
- ❖ Anjali Kaushik, Sailing Safe in Cyberspace 234-67(2013)
- ❖ I G.Ram Kumar, Cyber Crimes: A primer on Internet Threats and Email abuses 104-43(2006)
- ❖ Majid Yar, Cybercrime and Society 87-90(2006)
- ❖ Andrew Jones, Phishing Detection: A Literature Survey, 5-6(2013)
- ❖ Sanjay Bahl, Annual Report Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics & Information Technology Government of India (2018)
- ❖ I G.Ram Kumar, Cyber Crimes: A primer on Internet Threats and Email abuses 87-90 (2006)
- ❖ Mukesh bhardwaj, India among top three countries most targeted for phishing, THE INDIAN EXPRESS(May 25, 2013),<https://indianexpress.com/article/india/india-among-top-three-countries-most-targeted-for-phishing-says-report-5190826/>
- ❖ David jevans, APWG ,Unifyingthe global response to cybercrime (Sep 25,2018)<http://docs.apwg.org/wordphish.html>



LEGALITY OF DIGITAL SIGNATURE- A CRITICAL APPRAISAL

Ms. V. Vijaya Lakshmi,

*Research Assistant, Damodaram Sanjivayya National Law University, Visakhapatnam,
Andhra Pradesh*

Introduction:

A digital signature can be thought of as a digitized mark of approval, and is equivalent to a signature made with pen and paper. Digital signature software gives businesses the ability to collect these legally recognized signatures with more speed and efficiency. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. Furthermore, the ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. It is commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. Digital signatures play a vital role in the organizations since this technology enables the businesses to reduce the human errors, ultimately minimizes the paper work.¹

Digital signatures enable the businesses to manage their monetary subsidiary and cost of paper work. In addition, these signatures help the companies in proving that they are utilizing the green policies and ecofriendly procedures by cutting back the use of paper. This vast technology even reduces the time consumed in sending numerous emails and documents, since the entire work is entitled in few moments. The corporations prove their sharp time management skills through this technology. As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory.²

Digital signature:

Just the role the 'stamps', 'seal' or 'signature' play in traditional system to create the authentication of paper document, the digital signature plays the role to authenticate the electronic record. It establishes the authenticity of any electronic record which subscriber of digital signature wants to be authenticated the electronic record by affixing his digital signature. Digital signature in facts has two asymmetric pair of private and public key unique to each subscriber. The private key and public key are corresponding to each other in such a way that the electronic record encrypted with the help of any private key can be decrypted only with the help of corresponding public key.

¹ http://www.abhinavjournal.com/images/Management_&_Technology/Mar13/13.pdf

² Rohas Nagpal, President, Asian School of Cyber Laws, Simple Guide to Digital Signatures, E-book.



This digital signature creates digital ID for the subscriber holding digital signature certificate. This certificate is issued by Controller of Certifying Authority after due verification and adopting procedure. This certificate contains basic information about the person holding it. The information such as, the name, public key, place of working, date of issuance, date of expiry of the certificate and name of the Certification Authority. The certificate is also publicly made available through the directories or public folders on Web Pages. The law specifically made it clear that Controller will act as a repository for all Digital Signature Certificates issues under the Act and maintain a computerized database of all public keys in such a manner that such database and the public keys are available to any member of the public.¹

Meaning of Digital Signature:

A person's name written in a distinctive way as a form of identification in authorizing a Cheque or document or concluding a letter: 'the signature of a senior manager'²

Definition of Digital Signature:

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications³.

Binary code that, like a handwritten signature, authenticates and executes a document and identifies the signatory. A digital signature is practically impossible to forge and cannot be sent by itself but only as a part of an electronic document or message. In the US, electronic confirmation of signatures is legally acceptable from October 1, 2000 under the 'Electronic Signatures in Global and National Commerce Act' (also called 'E-sign Act'). The act gives full legal weight to electronic technologies that ensure authentication, confidentiality, data integrity, and non-repudiation, and directs courts to consider the electronic records on the same legal footing as the paper records.⁴

What are digital signatures?

Digital signatures are like electronic "fingerprints." In the form of a coded message, the digital signature securely associates a signer with a document in a recorded transaction. Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance. They are a specific signature technology implementation of electronic signature (e Signature)⁵.

History of Digital Signature:

¹S 20 of the Information Technology Act,

² <https://en.oxforddictionaries.com/definition/signature>

³<https://searchsecurity.techtarget.com/definition/digital-signature>

⁴ Read more: <http://www.businessdictionary.com/definition/digital-signature.html>

⁵ <https://www.docuSign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq>



Many people are under the false impression that digital signature technology is some new; the truth is that digital signatures have been around for decades, and they are gaining popularity in the mainstream.

Here are some of the milestones in the history of digital signature technology¹:

1976: Whitfield Diffie and Martin Hellman first described the idea of a digital signature scheme, but they only theorized that such schemes existed

1977: Ronald Rivest, Adi Shamir and Len Adleman invented the RSA algorithm, which could be used to produce a kind of primitive digital signature

1988: Lotus Notes 1.0, which used the RSA algorithm, became the first widely marketed software package to offer digital signatures

1999: The ability to embed digital signatures into documents is added to PDF format

2000: The ESIGN Act makes digital signatures legally binding

2002: SIGNiX is founded and becomes the most broadly used cloud-based digital signature software.

2008: The PDF file format becomes an open standard to the International Organization for Standardization (ISO) as ISO 32000. Includes digital signatures as integral part of format.

Today, digital signatures are well established as the most trusted way to get documents signed online. Unlike the original digital signature technology, today's digital signatures are easy to use and can be created using any computer with an Internet connection.

A digital signature scheme consists of three algorithms:

1. A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
2. A signing algorithm that, given a message and a private key, produces a signature.
3. A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.²

Electronic signature and a digital signature:

An electronic signature is any author identification and verification mechanism used in an electronic system. An electronic signature, also known as an e-signature is an electronic means that indicates that a person adopts the contents of an electronic message and that the person

¹<http://visual.ly/history-digital-signatures>

²https://en.wikipedia.org/wiki/Digital_signature



who claims to have written a message is the one who wrote it and that the message received is the one that was sent.¹

A digital signature is a type of electronic signature. It is a signature generated by a computer for a specific document, for the purposes of strong authenticity verification. Digital signatures are used in e-commerce and in other areas, as they are more secure than simple electronic signature.²

The difference between a digital signature and an electronic signature:

The broad category of electronic signatures (eSignatures) encompasses many types of electronic signatures. The category includes digital signatures, which are a specific technology implementation of electronic signatures. Both digital signatures and other eSignature solutions allow you to sign documents and authenticate the signer. However, there are differences in purpose, technical implementation, geographical use, and legal and cultural acceptance of digital signatures versus other types of eSignatures.³

In particular, the use of digital signature technology for eSignatures varies significantly between countries that follow open, technology-neutral eSignature laws, including the United States, United Kingdom, Canada, and Australia, and those that follow tiered eSignature models that prefer locally defined standards that are based on digital signature technology, including many countries in the European Union, South America, and Asia. In addition, some industries also support specific standards that are based on digital signature technology.⁴

An electronic signature means authentication of an electronic record by a subscriber by means of electronic techniques. An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

Digital signatures go beyond electronic versions of traditional signatures by invoking cryptographic techniques to dramatically increase security and transparency, both of which are critical in establishing a trust and legal validity. As an application of public key cryptography, digital signatures can be applied in many different settings, from a citizen filing an online tax return, to a procurement officer executing a contract with a vendor, to an electronic invoice, to a compliance officer signing an audit log or a software developer publishing updated code. Multiple technologies are available for creating and verifying digital signatures.

¹ <https://www.quora.com/Are-an-electronic-signature-and-a-digital-signature-similar>

² Ibid

³ <https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq>

⁴ Ibid



Digital Signatures have very specific benefits:¹

Authentication: SIGNiX provides various ways to identify a signer (from email verification to a text message to so-called knowledge-based authentication) so those persons cannot later say they did not sign the document.

Non-repudiation: SIGNiX walks users through a series of steps to sign a document and tracks all of those steps. Doing so eliminates the possibility of a signer suggesting they made a mistake in signing or never 'clicked' a button.

Integrity: Documents signed with SIGNiX alert the reader in real-time if anything has been changed or if there's any reason not to trust the document. Freely available PDF viewers provide this functionality on- of off-line.

In addition to improved security, digital signatures provide the following advantages:²

1. No need to print out documents for signing;
2. Reduced storage of paper copies;
3. Improved management and access (anytime/anywhere) of electronic versus paperdocuments;
4. Elimination of need for faxing or overnight mailing—reduction of cycle time;
5. Improved security of document transmission; and
6. Enhanced management processes outside the “final signature” step.

E-Signatures, based on digital signature technology, legally valid:

Yes, e-signatures are legally valid in India. In fact, e-signatures have been recognized by the Indian law, with the passage of the Information Technology Act in year 2000.

As per the IT Act, two types of signatures have the same legal status as handwritten signatures. These primarily include³:

(i) Digital Signatures: In this case, the signer is issued a long-term (1 to 2 year) certificate based digital ID stored on a USB token that can be used along with a personal PIN to sign a document.

Note: Previously, the signer was issued a long-term (1 to 2 year) certificate based digital ID stored on a USB token that could be used along with a personal PIN to sign a document digitally. Now with Aadhaar, that complicated procedure is not required anymore. You can simply use SignEasy's Aadhaar eSign to create a digital signature on the fly using your Aadhaar ID

(ii) Electronic signatures: These electronic signatures combine Aadhaar identity number with an electronic Know-Your-Customer (eKYC) method (which includes sending an One-Time-Passcode to the mobile number linked to the Aadhaar card for verification)

These Aadhaar based e-signatures and digital signatures are valid as long as they satisfy these conditions:

¹<https://www.signix.com/blog/bid/93731/How-Does-it-Work-Digital-Signature-Technology-for-Dummies>

² See also: ABA digital signature guidelines Industry standards[edit]

³ <https://www.quora.com/Is-electronic-signature-legally-binding-in-India>



(i) Electronic signatures must be uniquely linked to the person signing the document. (in the case of Aadhaar based signatures, they are linked by the unique Aadhaar ID)

(ii) At the time of signing, the signatory must have control over the data used to generate the electronic signature (for eg: they should be able to directly affix the electronic signature to the document)

(iii) There should be an audit trail of the steps taken during the signing process

(iv) In the case of digital signatures, signer certificates must be issued by Certifying Authority recognized by the Controller of Certifying Authorities appointed under the IT Act.

Few of the exceptional cases in which documents cannot be signed electronically and must be executed using traditional handwritten signatures include:

(i) Negotiable instruments such as a bill of exchange or a promissory note

(ii) Powers of attorney

(iii) Trust deeds

(iv) Wills and any other testamentary disposition

(v) Real-estate contracts such as leases or sales agreements.

Advantages and disadvantages of Digital Signature:

Advantages

1. With the use of digital signature, we can eliminate the possibility of committing fraud because the digital signature cannot be altered. Moreover, the forging signature is impossible.
2. By having a digital signature, we are proving the document valid. We are assuring the recipient that the document is free from forgery or false information.
3. Using a digital signature satisfies some type of legal requirement for the document in question. A digital signature takes care of any formal legal aspect of executing the document.
4. Includes an automatic date and time stamp, which is critical in business transactions.
5. Increases the speed and accuracy of transactions.
6. Digital signatures are a computerized form of signature that verifies that a package was sent by a certain individual or business, or that the right person actually signed a document. These signatures are secure and legal, and they can greatly improve your security¹.

Disadvantages

1. Cost-You must have the necessary software to encode the signatures, and if you are using hardware so that customers can sign physically, then the cost goes up even further. Digital signatures are additional cost that should be weighed against their potential security benefits.

¹[http://scienceandnature.org/IJEMS-Vol3\(2\)-Apr2012/IJEMS_V3\(2\)6.pdf](http://scienceandnature.org/IJEMS-Vol3(2)-Apr2012/IJEMS_V3(2)6.pdf)



2. Training and troubleshooting -If your employees are not sure how to use a digital signature, then you will have to spend time training them about how the signature process works. This will take them away from their jobs, costing you money. Additionally, as with all computer related applications, eventually, there will be hiccups in the system and you will need someone to troubleshoot. If none of your employees can find and fix the problem, you will have to hire someone else to do it¹.
3. Necessity-Digital signatures are a great security feature, but that does not mean they are a necessary one. If you own a law firm that deals in confidential materials, you might want to invest in a digital signature application for your clients. However, if you own a small family business that deals primarily in cash, you probably do not need it.
4. Technological Compatibility - refers to standards and the ability of one digital signature system to "talk" to another. It is difficult to develop standards across a wide user base.
5. Security Concerns - These efforts are perpetually hampered by lost or borrowed passwords, theft and
6. Tampering, and vulnerable storage and backup facilities.
7. Legal Issues - There is clear consensus that digital signature should be legally acceptable. However, many questions remain unanswered in the legal arena.

The advantages greatly overshadow the disadvantages. Practically the only disadvantages of using digital signature are the weak laws regarding cyber security which might cause any unnecessary hassles in case of a court case and that both parties have to purchase the certificates for the digital signature in order to use it instead of the one party courier charge. To conclude, without much argument, safely say that digital signature is a big breakthrough in the field of technology and can be used, nay, should be used generously as its advantages greatly overshadow their disadvantages.

Digital Signature Laws in India

Digital signature is electronically generated and can be used to make sure the veracity and legitimacy of data. The dawn of information technology revolutionized the whole world; India is not an exception to it; as technological activism is the social behavior in India.

IT Act Provisions Related to Digital Signature

Section 3 of IT Act, made the provision for it as: Authentication of electronic records.-

(1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

In IT Act, chapter 3 related to electronic governance, sections 4 and 5 are quite relevant.

Section 4 made the provision for Legal recognition of electronic records — where any law provides that information or any other matter shall be in writing, typewritten or printed form

¹ ibid



then not withstanding anything contained in such law, given requirement shall be deemed to have been satisfied if such information or matter is—

- (a) Rendered or made available in an electronic form; and
- (b) Accessible so as to be usable for a subsequent reference

Section 5 Legal recognition of [electronic signatures] — where law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of [electronic signatures] affixed in such manner as may be prescribed by the Central Government.

The Indian Evidence Act and Digital Signature

After the IT Act 2000, it was necessary to make an applicable amendment in the Indian Evidence act, to make it compatible.

Section 3 in the definition of “Evidence”, for the words “all documents produced for the inspection of the Court”, the word “all document including electronic records produced for the inspection of the Court”

Section 47A, says when the court has to form an opinion as to the digital signature or any person, the opinion of the certifying authority which has issued the Digital Signature Certificate is a relevant fact. It means while drawing the conclusion, court gives the weight of the digital signature as a relevant fact.

Further 67A proof as to digital signature – except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.

Section 85B exhibits the positive presumption as Presumption as to electronic records and digital signatures.- (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates¹.

Digital Signatures and the Indian Penal Code 1860

Indian penal code 1860 (IPC) is in operation in India very successfully for the last 158 years. Nobody seriously felt the need for an amendment because of its excellent draughtsman ship. However, a need was felt for addition of certain provisions to take care of the new developments in the field of electronics and information technology. Thus through the Information Technology Amendment Act 2008 IPC was also amended. The salient features of the amendments are discussed below.

Section 73A has been inserted to provide the same provision as in section 47A of the Indian evidence Act discussed above in this article. Section 464 has also been amended to provide that

¹ Indian Evidence Act 1872



the said section shall be made applicable to electronic records and electronic signatures also. Section 464 deals with situations when a person is said to make false document or electronic record. Section 466 provides for forging of electronic records also.

Conclusion:

Digital signature technology was developed in part to address the authentication needs of companies and consumers as they engage in transactions online. The growing online transactions and contracts requires stronger protection, which is currently fulfilled by digital signature. As electronic commerce develops and authentication becomes more important, consumers and companies will probably rely on digital signatures more often than they do now. However, it would be in the interest of cyber community if the government allows and intimate multiple method of authentication like the use of fingerprint or Aadhaar card linked with password based online transaction. The multiple methods would permit easy identification of persons which will assist in curbing online fraud and ease online transaction and further enhance online security of users as to even today the factual identity of persons online is a mirage.



CONSUMER PROTECTION IN E-COMMERCE: ISSUES AND CHALLENGES IN INDIA

Mr. M.A. Saleem Ahmed,

Research Scholar, Vels Institute of Science, Technology and Advanced Studies, Pallavaram,

Chennai, Tamil Nadu

&

Prof. Dr. Dilshad Shaik,

Research Guide, Vels Institute of Science, Technology and Advanced Studies & Dean,

Sathyabama School of Law, Chennai, Tamil Nadu

INTRODUCTION

E-Commerce is one of the utmost vibrant aspect in India brought a transformation in the life style of Indian consumers with the arrival of online retailers like Flip kart, Amazon and online auctioneer E-Bay in 1990's. After the entry of these online retailers some advanced phases were presented by the commercial and professional groups for promoting their business and profession by making use of network for posturing their products. E-Commerce however not specifically defined in any consumer legislation, is in general parlance defined as activities that relate to purchasing and selling of goods and services over the Internet. The scope of e-commerce has developed simultaneously with development of internet worldwide. The massive stage that e-commerce has provided the Indian traders for trade and commerce is noteworthy. Internet has therefore revolutionized the way Indians and the rest of the world purchase and sells their products. On one hand online shopping entryways like Flipkart and Jabong ensure numerous alternatives for a wide range of merchandise online with brisk and effective delivery systems, then again, online operations are undertaken by Indian railroads, State Electricity Boards, banks, movie theaters etc. for payment and booking purposes. In this way the feasibility of operations that online transactions have achieved to the Indian trade industry and other industry is remarkable. However, the miserable reality on the other side of the coin is that even with such increased scope, there is a disadvantage of entering into such online transactions, being the equivocality in the laws relating to them. It commonly uses electronic communications technology, for example, the Internet, extranets, e-mail, e-books, database, and mobile phones.

GROWTH OF E- COMMERCE IN INDIA

E-Business in India has undergone a tremendous development yet at the same time it has a fragment of barriers which are the obstacles in the method for E-business. It needs a concentration and ought to be prioritize to make the nation in the lines of E-Business.



Types of E-Commerce:

B2B E-Commerce: Companies working with each other, for example, manufacturers selling to merchants and wholesalers selling to retailers. Evaluating is based on amount of order and is often negotiable.

B2C E-commerce: Businesses selling to the general public through catalogues using shopping carrier software. By dollar volume, B2B takes the prize, however B2C is really what average people has at the top of the priority list with regards to e-commerce as a whole. For example, indiatimes.com.

C2C E-Commerce: There are numerous sites offering free classifieds, closeouts, and gatherings where people can purchase and sell on account of online payment system like PayPal where people can send and receive money online effortlessly.

G2E (Government-to-Employee), G2B (Government-to-Business), B2G (Business-to-Government), G2C (Government-to-Citizen), C2G (Citizen-to-Government) this all are types of ecommerce that involve transactions with the government- - from procurement to recording taxes to business registrations to renewing licenses¹.

Status of E-Commerce in India

Ever since the entry of E-commerce in India it has become an integral part of our daily life. There are some websites providing any number of goods and services. These Indian E-commerce gateways provide goods and services in various category, for example:

- Auto-mobiles- On these sites one can purchase and vend four wheelers and two wheelers, new as well as used vehicles, online. Some of the services they provide are: car research and reviews, online assessment, technical stipulations, automobile insurance, automobile finance.
- Stocks and Shares- In India today, one can even deal in stocks and shares through e-commerce. Some of the services offered to registered members are: Online purchasing/vending of stocks and shares, Market analysis and research, Company information, Comparison of companies, Research on Equity and Mutual funds.
- Real estate - They provide information on new properties as well as for resale. One can deal directly with developer through consultant. Allied services: Housing finance, Insurance companies, Architects and Interior Designers, NRI services, Packers and Movers.
- Travel and Tourism- They provide tourist destination sites are categorized according to themes like: Adventure-trekking, mountain climbing etc.².

¹Sarbapriya Ray, *Emerging Trends of E- Commerce in India: Some Crucial Issues, Prospects and Challenges*, IJBMI JOURNAL, 2011, at 17, 20

²Dr. Rajeshwari M. Shettar, *Emerging Trends of E- Commerce in India: An Empirical Study*, INTERNATIONAL JOURNAL OF BUSINESS AND MANAGEMENT INVENTION, 2016, at 25, 31



Governmental Regulation

Asia Pacific Economic Cooperation (APEC) was established in 1989 with vision of achieving stability, security and prosperity for the region through free and open trade and investment. APEC has an Electronic commerce staring Group as well as working on common privacy regulations throughout the APEC region. Internationally there is the International consumer protection and Enforcement Network (ICPEN), which was formed in 1991 from an informal network of government customer fair trade organisations. The purpose was stated as being to find ways of cooperating on tackling consumer problems connected with cross-border transactions in both goods and services, and to help ensure exchanges of Information among the participants for mutual benefit and understanding¹.

Barriers to E-commerce in India

- Payment collection-When the consumer pays the amount through net banking the company end up giving a significant share of revenue (4% or more) even with a business of thin margin. This effectively means the company give away with almost half of profits².
- Logistics- you should deliver the product, safe and secure, in the hands of the right person in right time. Regular post doesn't offer an acceptable services and couriers have high charges and limited reach. Initially, you might have to take insurance for high value shipped articles increasing the cost.
- Vendor Management- Vendor will have to come down and deal in an inefficient system for inventory management. This will slow down drastically. Most of them won't carry any digital data for their products.
- Taxation- Octroy, entry tax, VAT and lots of state specific forms which accompany them. This can be confusing at times with lots of exceptions and special rules³.

E – COMMERCE AND CONSUMER RIGHTS: APPLICABILITY OF CONSUMER PROTECTION LAWS IN ONLINE TRANSACTIONS IN INDIA

CONSUMER PROTECTION ACT, 1986

Normally a consumer has various rights that are granted to him by the provisions of numerous consumer laws enacted in India. Consumer Protection Act, 1986 is the fundamental and principle legislature that lays down and guarantees various rights to the persons who act as consumers. This Act enumerates the three-tier mechanism that exists in India namely at the district, state and national levels to redress any consumer dispute. However, there was no any

¹Dr. Rajeshwari M. Shettar, *Emerging Trends of E- Commerce in India: An Empirical Study*, INTERNATIONAL JOURNAL OF BUSINESS AND MANAGEMENT INVENTION, 2016, at 25, 34

² PROF. ALTAF KHAN, GLOBAL TRENDS IN E-COMMERCE 305-306 (1ed. 2011)

³Kiranmayi. N, *A Study on Barriers to E- Commerce in India*, INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING AND TECHNOLOGY, 2016, at 335, 336



specification and it was ambiguous as to whether such provisions would be applicable to online transactions. On July 8, 2014 the Minister of state for Consumer Affairs, Food and public Distribution, in a written reply in Lok Sabha made an announcement of including online transactions also in the ambit of Consumer Protection Act, 1986. This inclusion in consumer protection Act fundamentally meant that complainants can approach various consumer Forum i.e. District Consumer Forum, State Commission and National Commission For resolution of their grievances. Though such an announcement does not necessarily transform into a law, it was a vital step to bring into effect, a mechanism for safeguarding the rights.

In effect the provisions of the Consumer Protection Act, 1986 are made applicable to online transactions as well. Prior to this recent express declaration, the Consumer Protection Act, 1986 was impliedly applied to online transactions, in accordance with the definitions provided under the Act. Any person who buys any good or avails or hires any service for any consideration, whether paid or otherwise, except for commercial use is regarded as a consumer under the Consumer Protection Act, 1986. Buyer as per Sale of Goods Act, 1930 is defined as any person who buys or agrees to buy goods. Thus following these two definitions, any person who pays or agrees to pay a price for a particular good can be regarded as a consumer, irrespective of such a sale being online. Additionally, contract of sale as defined under the Sale of goods Act, 1930 is indicative of the fact that such may apply to online transactions along with regular transactions. Thus, earlier though there was absolutely no express mention of e-commerce falling under the ambit of Consumer Protection Act, 1986 these provisions impliedly provided a right to consumer to seek redressal under the same. However, Consumer Protection Act, 1986 only provides a narrower picture.

The Act does not provide a solution to the various loopholes that are brought about by online transactions due to their impersonal nature, which may be considered their flipside as well. The scope that Consumer Protection Act, 1986 has with respect to e-commerce is thus restricted to providing a redressal mechanism that is applicable to direct transactions as well.

Further, Consumer protection Act, 1986 becomes applicable when there is a “defect in goods” or “deficiency in services”. Hence only if one of the above two criteria are satisfied consumer protection Act, 1986 would come into play. However, there is no redressal provided if goods are not delivered in the time specified. Such things create more trouble to the online consumers due to the anonymity of the seller. Many complaints have been filed by online consumers regarding the same in consumer forums, however the unclear laws and the consequent ambiguity has resulted in their grievances not being paid.

INFORMATION TECHNOLOGY ACT, 2000

Aside from the guideline law for Consumer Protection, numerous different laws cover online transaction. Information Technology Act, 2000 is another utilitarian and far reaching enactment which gives a legitimate system to web-based business. It essentially covers commercial



transactions, in specific between the government through of its many functionaries and the citizens. The transactions are focused towards e-governance and are aimed at implementing measures for authentication of the electronic records by usage of digital signature certificates etc for carrying out day to day business transactions like filing and viewing official documents in the electronic format. The IT Act, 2000 is an attempt by the govt. to digitalize its workings by making every piece of information available online and further ensuring that such transactions are secured. Further, it provides remedial measures for the E-consumers. The following provisions of Information technology Act deals with protection of e-consumers.

Validity of E-Contracts

Electronic contracts are governed by the basic principles provided in Indian contract Act, 1872, Section 10A of the Information Technology Act, 2000 provides validity to e-contracts. The Supreme Court in Trimex International FZE Ltd. Dubai v. Vedanta Aluminium Ltd¹. Has held that e-mails exchanges between parties regarding mutual obligations constitute contract.

Data protection

Security of the information provided during the online transaction is a major concern², the intermediaries have the obligation to publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person. Such rules and regulations must inform the users of computer, display, upload, modify, publish, transmit, update or share information. Also, the intermediary must not knowingly host or publish any prohibited information and if done, should remove them within 36 hours of its knowledge. In Consim Info Pvt. Ltd v. Google India Pvt. Ltd³, the Delhi Court Google had extended the argument that being search engine, they cannot control the fact whether some website, any advertisement given on their site is genuine or fraud. The court then observed that though the intermediary, Google, cannot be made liable for infringement arising out of a third party's actions since it is not possible to always check every advertisement posted online; however, it was said that as per section 3(4) of the aforesaid Intermediaries Guidelines, Google had to act upon it within 36 hours of receipt of such complaint, failing which it may be held liable. This issue is also in no way different from the issues time and again raised by the public at large in other than e-commerce when their phone numbers are given by banks etc. For tale marketing and other unwanted calls and SMS from business groups. This issue can very well be handled alleging the wrong doer for deficiency in services and unfair trade practices under Consumer Protection Act.

Yet, this act does not holistically cover all the aspects of e-commerce with respect to consumer rights. It primarily covers business or commercial transactions that are undertaken by business

¹Trimex International FZE Ltd. Dubai v. Vedanta Aluminium Ltd (2010) 1 SCALE 574

²The Information Technology (Intermediaries Guidelines) Rules, Section 43A, 2011

³Consim Info Pvt. Ltd v. Google India Pvt. Ltd (2013) 54 PTC 578 (India)



to govt. or vice versa. It provides details about filing, retaining, viewing documents with respect to a business and safeguards and authenticates those documents with the help of digital signatures, asymmetric crypto system etc. An ordinary Indian man does not, in his daily life enter into such transaction; instead they mostly utilize electronic commerce for online shopping, online banking and money transfer activities etc. No specific provisions for the same have been laid down under the Act even though it is the need of the hour for the enactment of such provisions. The objectives of the Act as stated include facilitation and giving legal sanction to electronic fund transfers between banks and financial institutions in addition to giving legal recognition for keeping of books of accounts by bankers in electronic form. Though nowadays such facilities have been made possible, no legal framework for protection of consumer rights is provided under the IT Act. Thus, this significant aspect of e-commerce is not covered¹.

CONSUMER PROTECTION (AMENDMENT) BILL, 2015

The Consumer Protection Act, 1986 may be replaced by the new Consumer Protection Bill 2015 that will also incorporate e-commerce. This proposed bill could replace the 29-year-old law and recognise the growing complexity of the business landscape with the expansion of e-business across India. Due to incredible increase in the acceptance of e-commerce, the proposed amendment attempts to include e-commerce transactions under the ambit of the Act.

The bill sets up a new regulatory authority that will have powers to recall goods and services and also initiate class action lawsuits against companies that are defaulting against the statutes of the law and these will now, explicitly, include Indian e-commerce companies. Under the current Consumer Protection Act, a consumer can initiate legal action against a seller only in the place where transaction takes place. The new Bill contains an enabling provision for consumers to file grievances electronically, and in consumer courts that have jurisdiction over the place of residence of the complainant.

CONCLUSION

A developing country can become industrialized and modernized if it can extensively apply IT to enhance productivity and international competitiveness, develop ecommerce and e-governance applications. Many countries in Asia are taking advantage of E-commerce through opening of economies, which is essential for promoting competition and diffusion of Internet technologies. In the next 3 to 5 years, India will have 30 to 70 million Internet users² which will equal, if not surpass, many of the developed countries. Internet economy will then become more meaningful in India. With rapid expansion of internet, E-commerce, is set to play a very important role in the 21st century, the new opportunities that will be thrown open, will be accessible to both large

¹Kanika Satyan, *E-Commerce And Consumer Rights: Applicability of Consumer Protection Law in Online Transactions In India*, (Mar.10, 2016, 11.00AM), file:///C:/Users/VS/Downloads/SSRN-id2626027.pdf

²Kanika Satyan, *E-Commerce And Consumer Rights: Applicability of Consumer Protection Law in Online Transactions In India*, (Mar.10, 2016, 11.00AM), file:///C:/Users/VS/Downloads/SSRN-id2626027.pdf



commerce so that while domestic and international trade are allowed to expand their horizons, basic rights such as privacy, intellectual property, prevention of fraud, consumer protection etc. are all taken care of. Discussions are ongoing in the country to allow FDI in e-commerce transactions in India. This illustrates the level of importance that e-commerce has achieved in the Indian trade industry. It has not only made lives of consumers simple but has also ensured that the traders are able to sell their products worldwide, without any hassles. The only dilemma remains in the fact the Indian legal system does not cover the facet relating to consumer rights in case of e-commerce. Thus, the vital need of the hour is to provide for express declaration of laws that would make e-commerce hassle free and this would in turn encourage more people to resort to commerce through the internet.

REFERENCES

Book:

1. PROF. ALTAF KHAN, *GLOBAL TRENDS IN E-COMMERCE* (1ed. 2011).

Journals:

2. Sarbapriya Ray, *Emerging Trends of E- Commerce in India: Some Crucial Issues, Prospects and Challenges*, IJBMI JOURNAL, 2011.
3. Dr. Rajeshwari M. Shettar, *Emerging Trends of E- Commerce in India: An Empirical Study*, INTERNATIONAL JOURNAL OF BUSINESS AND MANAGEMENT INVENTION, 2016.
4. Kiranmayi. N, *A Study on Barriers to E- Commerce in India*, INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING AND TECHNOLOGY, 2016.

Case Laws:

1. Consim Info Pvt. Ltd v. Google India Pvt. Ltd (2013) 54 PTC 578 (India)
2. Trimex International FZE ltd. Dubai v. Vedanta Aluminium Ltd (2010) 1 SCALE 574

Acts:

1. The Information Technology Act, 2000
2. The Information Technology (Intermediaries Guidelines) Rules, 2011
3. The Indian Contract Act, 1882
4. The Consumer Protection Act, 1986
5. The Sale of Goods Act, 1930

Website:

Kanika Satyan, *E-Commerce and Consumer Rights: Applicability of Consumer Protection Law in Online Transactions in India*, file:///C:/Users/VS/Downloads/SSRN-id2626027.pdf



CONTRACTING IN CYBER SPACE: CRITICAL ANALYSIS OF LEGAL REGULATIONS OF
E-CONTRACTS IN INDIA

Ms. Shanthi Samandha K.,

*Assistant Professor (Law), Andaman Law College, Transport Bhawan, Andaman & Nicobar
Islands.*

INTRODUCTION

Contracts form the back bone for all kind of commercial activities. For any kind of transaction starting from petty business to multinational trade, contracts form the foundation or the primary start of such commercial activity. The recent revolution in technology has brought a wider option for people to trade on line. It has drastically changed the life styles of the people. E-commerce has broken the traditional way of trading, in fact it has connected people through east to west and north to south. It saves time and money in meeting people and making contracts. E-commerce is nothing but buying and selling of various goods, products and data through a medium of computerized communication network. Developments and inventions of new technologies have made them as an essential part of the commercial transactions. People can buy and sell things in just a click without spending time. Many e-services like e-banking, e-ticketing, e-bill payments etc. have reduced the burden of people at both the end. In India the concept of e-commerce has grown gradually since last few years, now the number of people availing the facilities on electronic transaction is high. E-commerce is replacing the traditional commercial activities in a fast pace. This paper tries to trace the development of traditional contracts to e-contracts and tries to evaluate the legal provisions regulating such e-contracts in India.

NATURE OF E-CONTRACTS

E-contracts can be better understood by reading the general principles of a contract. A contract is defined under the Indian Contract Act 1872 as “An agreement enforceable by law is a contract”¹. It also explains the essentials of valid contract “All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void. Nothing herein contained shall affect any law in force in India, and not hereby expressly repealed, by which any contract is required to be made in writing or in the presence of witnesses or any law relating to the registration of documents”². The consideration and the object of the contract must be lawful³.

E-contracts have the same features of a normal paper contract, for e.g. if one of the contracting party drafts the contract and send it to the second party through e-mail, the second

¹ S.2(h), The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India).

² S. 10, The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India).

³ S. 23, The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India).



party receives the draft contract in his mail and approves it by attesting his electronic signature and sends back to the first party. Since a traditional ink signature isn't possible on an electronic contract, people use several different ways to indicate their electronic signatures, like typing the signer's name into the signature area, pasting in a scanned version of the signer's signature or clicking an "I Accept" button and many more¹. Hence there is no any fast and hard definition for e-contract. The traditional definition of contract cannot be applied strictly to 'e-contract', because the realm of e-contract is much bigger than the realm of traditional contract. To put it simply, e-contract is any contract which is entered in internet by competent parties, with lawful consideration, free consent, without any malafide intention and to create a legal relationship².

E-contracts facilitate transactions and agreements electronically without the parties meeting each other i.e. through electronic mode. E-commerce to succeed such contracts need to be validated legally an alternate mode of transaction through online using the latest technological developments³.

TYPES OF E-CONTRACTS

The E-Contracts are broadly divided into two kinds one is the common method is to enter into contracts by exchanging e-mails between the contracting parties and the other is the standard contracts in the websites.

CONTRACTS THROUGH E-MAIL

The drafting of the e-contracts are of the similar nature to that of the traditional contracts. The exchange of e-mails between the contracting parties serve as the letters used to communicate in a traditional contract. Such e-mail contracts have legal validity similar to that of the traditional contracts. A contract through email becomes a valid contract when the basic essentials of a contract is met i.e. offer and acceptance. It must also be evident to the courts that through the email exchanges, external conversations and surrounding circumstances, both parties intended to form and be bound by a contract⁴. If an e-mail or chain of e-mails clearly states an offer for entering into a deal with all of the material terms and the other side responds

¹H.P. Purvik, *Flaws in E-Contracts and E-Commerce: Better Implementation of Cyber Laws in India*, 1 IJRESM 502, 502 (2018).

² Ambika SP, *Legal Regulation in India an Indian perspective*, (Oct. 31, 2018, 11:01 AM), <http://hdl.handle.net/10603/38507>.

³ Singh R.K., *Understanding Electronic Contracts*, Chapter 3.

⁴ Kathleen Ready, *Email Contracts- Who, What, When and Where – The Formation of binding agreements through email exchanges*, Mondaq, (Oct. 31, 2018, 04:59 PM), <http://www.mondaq.com/australia/x/431732/Contract+Law/Email+contracts+Who+What+When+and+Where+The+formation+of+binding+agreements+through+email+exchanges>.



by e-mail accepting the terms, then there's a good chance that a valid contract has been formed – even though no signatures have been exchanged¹.

WEBSITE STANDARD CONTRACTS

Every websites have a standard contract to access the contents and services provided by the website. Whenever a person wants to access any information or services provided by any website he has to enter a standard contract.

Again the website standard contracts are further divided into three types:

a) BROWSE WRAP/WEB WRAP CONTRACTS

These contracts are published in a website only when these contracts are agreed by the user the contents of the website can be used. Browse-wrap (also Browser wrap or browse-wrap license) is a term used in Internet law to refer to a contract or license agreement covering access to or use of materials on a web site or downloadable product. In a browse-wrap agreement, the terms and conditions of use for a website or other downloadable product are posted on the website, typically as a hyperlink at the bottom of the screen².

In a US case where the *"Plaintiffs acted upon Defendant's invitation to download their free software, Smart Download. Because of the way Netscape had its download setup online, Plaintiffs were not required to read the full terms of the contractual agreement, including an arbitration clause, before they clicked the download button. The District Court found that the downloading of software did not constitute an acceptance of Defendant's terms because there was no reasonably conspicuous notice and because a reasonable internet user would not expect to submit to an arbitration clause upon installing a free download. Defendant appealed. The issue here is whether Plaintiffs will be held to an arbitration clause and contractual terms that were inconspicuous due to their online placement. The court found that "a consumer's clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms. Because the plaintiffs were not put on notice of these terms they were not bound by them"*³.

In *"Ticketmaster v. Tickets.com, the court looked at a breach of contract claim where the terms and conditions were situated at the bottom of the home page in "small print." The court ruled for the defendant in this case but did allow Ticketmaster to replead if there were facts showing that the defendant had knowledge of the terms and implicitly agreed to them"*⁴.

b) CLICK WRAP CONTRACTS

A click wrap contract is generally used for accessing software licences and online transactions. When a user wants to enjoy the software usage and online transaction services

¹ All Business Editors, *Can an E-mail Agreement Be a Binding Contract?*, AllBusiness, (Oct. 28, 2018, 02:30 PM), <https://www.allbusiness.com/can-an-e-mail-agreement-be-a-binding-contract-2378-1.html>.

² *Kwan v. Clearwire Corp.*, No. C09-1392JLR, 2012 WL 32380 (W.D. Wash. Jan. 3, 2012).

³ *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2nd Cir.2002).

⁴ *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 WL 525390, at *3 (C.D.Cal. March 27, 2000).



then he must agree to the terms and conditions of the related click wrap contracts. A click wrap or click through agreement is a digital prompt that offers individuals the opportunity to accept or decline a digitally-mediated policy¹. Privacy policies, terms of service and other user policies, as well as copyright policies commonly employ the click wrap prompt. Clickwraps are common to signup processes for social media services like Face book, Twitter or Tumblr, connections to wireless networks operated in corporate spaces, as part of installation processes of many software packages, or in other circumstances where agreement is sought using digital media².

In a US case the binding nature of the click wrap agreement has been discussed. *"Is an online click wrap agreement binding when an online user has been given reasonable notice of the agreement's term and it is clear that once the user clicks on the acceptance "button", the user agrees to be bound by those terms notwithstanding that the agreement does not include a specific price term, but describes with adequate definiteness, a practicable process by which price is determined?"*

"It was held that, yes. When an online user has been given reasonable notice of the agreement's term and it is clear that once the user clicks on the acceptance "button", the user agrees to be bound by those terms notwithstanding that the agreement does not include a specific price term, but describes with adequate definiteness, a practicable process by which price is determined, then the online clickwrap agreement becomes binding on the online user."

c) **SHRINK WRAP CONTRACTS**

Shrink wrap contracts are boilerplate or license agreements or other terms and conditions which are packaged with the products. The usage of the product deems the acceptance of the contract by the consumer. The term 'Shrink Wrap' describes the shrink wrap plastic wrapping which coats software boxes or the terms and conditions which come with products on delivery⁵.

The legal status of shrink wrap contracts in the US is somewhat unclear. In the 1980s, software license enforcement acts were enacted by Louisiana and Illinois in an attempt to address this issue, but parts of the Louisiana act were invalidated in *Vault Corp. v. Quaid*

¹Obar, Jonathan A.; Oeldorf-Hirsch, Anne (2018). "The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media". *Social Media + Society*. **4** (3). Retrieved 19 July 2018.

²*Clickwrap*, Wikipedia, (Oct. 29, 2018, 11:23 AM) https://en.wikipedia.org/wiki/Clickwrap#cite_note-SMS-1.

³ *Feldman v. Google, Inc.* United States District Court for the Eastern District of Pennsylvania 513 F.Supp.2d 229 (2007).

⁴ *Giles, J., Feldman v. Google, Inc.* United States District Court for the Eastern District of Pennsylvania 513 F.Supp.2d 229 (2007).

⁵ Rebecca Furtado, *E-Contracts- What are Shrink Wrap, Click Wrap and Browse-Wrap Agreements?*, IPleaders, (Oct. 22, 2018, 10:27 AM), <https://blog.ipleaders.in/e-contracts-shrink-wrap-click-wrap-browse-wrap-agreements/>.



Software Ltd.¹, and the Illinois act was quickly repealed. Case history also fails to clear up the confusion.

One line of cases follows *ProCD v. Zeidenberg*² which held such contracts enforceable³ and the other follows *Klocek v. Gateway, Inc.*,⁴ which found the contracts at hand unenforceable, but did not comment on shrink wrap contracts as a whole.

ISSUES OF E-CONTRACTING IN CYBER SPACE

A Contract forms the base for any trading or commercial activity. For a valid commercial activity a legally valid and enforceable contract must be concluded. An analysis of the activities such e-commerce and their e-contracts show its merits and demerits.

The growth of e-commerce activities has put the legislators under a great pressure to legislate a law with more vibrancy and effectiveness with a good regulatory mechanism, which would ultimately result in more e-commercial activity helping in the economic growth of the country. The rapid growth in the field of information technology has posed various challenges to the legal system all over the world.

The e-contracts though is similar in the valid essentials of the traditional contracts it has raised serious doubts in the mind of the people relating to the following:

a) IDENTIFICATION

The identification of parties is important for any contractual activity. In a traditional contract the parties to the contract are known to each other and the physical presence of the person is more evident for authenticity. Whereas in an E-contract in most of the cases the authenticity of the person is doubtful. The contract would be prevented by a mistake to the identity of the person. These kinds of problems are new but become worse in an online environment. Persons in online are always stranger to one another, there is an unimaginable physical gap between the parties and most of the information shared by them are not reliable.

Problems of identification are usually discussed in relation to attribution. Absent of statutory provisions or agreement, open electronic networks, do not change the basic principle of attribution: a person is responsible for the legal effects of an act, if he or she performed or authorized such act. Problems of attribution are therefore not Internet-specific⁵. In electronic commerce, the online nature of acceptances can make it relatively easy for identity forgers to

¹ 655 F. Supp.750, 761 (E.D.La.1987), aff'd, 847 F.2d 255 (5th Cir. 188), (Sep. 30, 2018, 03:25 PM)

http://itlaw.wikia.com/wiki/Vault_v._Quaid.

² 908 F. Supp. 640 (W.D. Wis. 1996), (Sep. 30, 2018, 03:45 PM)

http://itlaw.wikia.com/wiki/ProCD_v._Zeidenberg.

³ David L. Hayes, Esq., *The Enforceability of Shrink wrap Licence Agreements On-Line and Off-Line*, (1997), (Sep. 30, 2018, 04:15 PM), [http://euro,ecom.cmu.edu/program/law/08-732/Transactions/Shrinkwrap Fenwick.pdf](http://euro,ecom.cmu.edu/program/law/08-732/Transactions/Shrinkwrap%20Fenwick.pdf).

⁴ 104 F.Supp.2d 1332 (D.Kan. 2000), (Oct. 1, 2018, 8:45 PM), <http://www.law.unlv.edu/faculty/rowley/Klocek.pdf>.

⁵ A.H.Boss, *Searching for security in the Law of Electronic Commerce*, 592



pose as others. This situation can however be avoided by the use of electronic signatures to establish identity in online transactions.

b) ATTRIBUTION

Next to authenticity the serious question is about attribution. In an E-contract it is important to know that to whom the offer is attributed to. Very often data messages are generated automatically by computers without direct human intervention. The computers are programmed by the person (originator) to do this. These situations are also covered by the IT Act through the incorporation of the concept of attribution of electronic records¹.

“S.11: Attribution of electronic records.—An electronic record shall be attributed to the originator—

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.”

c) JURISDICTION

When we enjoy the cross border services of internet on the other hand there is a serious question and applicability of jurisdiction. As to which country law is applicable and the greatest challenge is to solve the issue of conflict of laws. Internet by nature can be accessed from any part of the world and hence it is multi-jurisdictional. When two different nationals enter into an E-contract and when a dispute arise the challenge is to determine the jurisdiction regarding which country has the jurisdiction to take up the matter, which country's law is applicable to determine the dispute. These are the difficulties faced by the courts worldwide because of the boundary less transactions. While most laws have territorial nexus, the internet defies the notion of territoriality³.

Generally all jurisdictional issues in India are resolved under the provisions of Code of Civil Procedure, 1908. Jurisdictional issues in India are determined either by the place of residence or place of business test or cause of action test⁴. The first test is an objective one and easy to determine. It is unlikely to pose any serious issue in e-commerce disputes. The cause of action test is a subjective test and is most likely to be debated in e-commerce cases⁵. The Information Technology Act says that the place of business shall be deemed as the place of

¹NandanKamat, *Law relating to Computers, Internet and Ecommerce*, 3rd edn.

² S.11, Information Technology Act, 2000, No.21, Acts of Parliament, 2000 (India).

³ Raman Mittal, *Dispute Resolution in Cyber Space; Determining jurisdictional and applicable law*, in S.K.Verma and Raman Mitta.

⁴ S.20, Code of Civil Procedure, 1908, No.5, Acts of Parliament, 1908 (India).

⁵Dr.Farooq Ahmed, *Cyber Law in India- Law on Interest*, 2nd edition.



dispatch or receipt of the electronic record as the case may be. The place where a contract is concluded will be either the place where acceptance is posted or where acceptance is received depending upon the medium of communication used.

LEGAL FRAMEWORK

The technology has proven a vast change in the lives of people, hence when people adhere and change strictly to the changes in the cyber world, it is the bound duty of the law to support and protect the people by bringing changes in law according to the need of the people. Companies in order to expand its business in a more effective manner keeps doing lots of research and frame new procedures and rules, but the legal system could not keep up the speed to that of the companies in order to legislate new laws according to the need of the hour, hence it is very feeble and vague on the applicability of these laws to the present scenario.

a) THE INDIAN CONTRACT ACT, 1872

The Indian Contract Act, 1872 governs the contractual activities in India, which has the main aim to define and amend certain parts of the law relating to contract¹. The provisions of the Indian Contract Act, 1872 are applicable to E-Contracts and the Information Technology Act grants legal recognition to the transactions carried out by means of electronic data interchange and other means of electronic communication².

The simplicity of the execution of an E-Contract being confounding, many sometimes wonder about its validity, especially when compared to a traditional written contract. The simple truth lies in the fact that the Indian Contract Act, 1872 has not specifically laid out any specific way of communicating an offer and what constitute its acceptance. The same can be achieved verbally, in writing or even through conduct. This shows that even in its simplicity, an E-Contract is as valid as a traditional written contract; the only condition/ requirement being that an E-Contract should possess all the essentials of a valid contract as under the Indian Contract Act, 1872³.

b) THE UNCITRAL MODEL LAW

The United Nations, UNCITRAL Model Law on E-commerce which was adopted by its signatories. The UN member states slowly started to legislate domestic laws basing the provisions of the UNCITRAL Model Law. In order to make the UNCITRAL Model Law on Electronic Commerce more effective the United Nations adopted another model law, the

¹ Preamble, The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India).

² Vijaysingh Shashikant Pisal, *Advantages of E-Contracts over Traditional Contracts: E-Contracts and E-Commerce in India*, (Nov. 1, 2018, 11:52 AM).

http://elib.bvuict.in/moodle/pluginfile.php/183/mod_resource/content/0/Advantages%20of%20E-Contracts%20over%20Traditional%20Contracts%20-%20E-Contracts%20and%20E-Commerce%20in%20India%20-%20Vijaysinh%20Shashikant%20Pisal.pdf.

³ Maneck Mulla, *Validity of Electronic Contracts in India*, Mondaq, (Nov. 1, 2018, 02:30 PM), <http://www.mondaq.com/india/x/699022/Contract+Law/Validity+Of+Electronic+Contracts+In+India>.



UNCITRAL Model Law on Electronic Signatures. As cyber law develops around the world, there is a growing realization among different nation states that their laws must be harmonized and international best practices and principles must guide implementation. Many countries are trying to establish harmonized legal regimes in order to promote online commerce¹.

“Leadership in telecommunications is also essential, since we are now in the age of e-commerce.”

Michael Oxley

Hence India must make sure in providing a better infrastructure for promoting e-commerce which forms as one of the important source of Indian Economy. It is essential, therefore, to create a policy and regulatory environment that favours the development of E-Commerce and harmonises national approaches in diverse areas such as telecommunications, trade, competition, intellectual property, privacy, and security².

c) THE INFORMATION TECHNOLOGY ACT, 2000

India being the signatory to the model law, it was required to enact a domestic law basing the UNCITRAL Model Law. After the advancement in technology in order to govern and regulate the activities in the cyber space the Information Technology Act, 2000 was enacted basing on the UNCITRAL Model Law on Electronic Commerce, which provides the infrastructure of E-Commerce. The Act aims to facilitate the development of a secure regulatory environment for electronic commerce by providing a legal Infrastructure governing electronic contracting, security and integrity of electronic transactions, the use of digital signatures and other issues related to electronic commerce³. Information Technology Act approves the validity of E-Contract as follows:

"S.10-A: Validity of contracts formed through electronic means- Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose."⁴

The Information Technology Act not only validates the E-Contracts but also addresses three main functions first the smooth E-Commerce transaction of business to business (B to B) and business to consumer (B to C). Second the smooth E-Governance transaction to Government to Citizen (G to C) and Citizen to Government (C to G). Third to prevent cybercrimes and regulate the functioning of internet.

¹PavanDuggal, *Harmonisation of E-commerce laws and Regulatory system in South Asia*, (Nov. 1, 2018, 10:30 AM), www.unescap.org.

²Diddar Singh, *Electronic commerce, issues of policy and strategy for India*.

³ Supra at 22.

⁴ S.10 A, Information Technology Act, 2000, No.21, Acts of Parliament, 2000 (India).



The main feature of the Information technology is the inclusion of the definition on electronic signature, which forms the very basic need for entering in to E-contracts.

“S.3A: Electronic signature.—(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which—

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if—

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfils such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.^{1”}

The provisions of Information Technology Act try to implement the above functions very effectively.

CONCLUSION

As there is a Himalayan growth in the field of technology and where almost everything has become digitalised the contracts entered in the cyber space must be taken utmost care

¹ S. 3A, Information Technology Act, 2000, No.21, Acts of Parliament, 2000 (India).



complying with all essentials of a valid contract. It should comply with all the legal requirements only by which it can be validated. The laws has been drafted in such a manner that it has been taken utmost care to solve almost all the issues arising out of the e-commerce and the e-contracts relating to the e-commerce. E-commerce is expected to extend the commercial activities across the global in even more fast pace, in such a situation it is the burden over the legislators to mould the present laws to support such E-commerce activities in a better manner.



A CRITIQUE OF CYBER LAW IN INDIA

Dr. E. Ajitha

Assistant Professor, Department of Bank Management

Ethiraj College for Women (Autonomous)

Introduction

The Information and Communication Technology (ICT) enabled communication has a tremendous impact in the 21st century and has replaced the traditional ways of not only how individuals interact and communicate with each other but also how they do business in this knowledge economy. It has been also instrumental for the growth and development of trade and commerce across the globe. In India it is estimated that around billion people use the internet on a regular basis for various reasons and needs. The government initiative on cash less payments is a great push in enabling the ICT based transactions in every corner of India both urban and rural. As has been witnessed in the history of man, every time science and technology progresses, there has been a consequential occurrence of newer crime committed by people by use of technology. ICT is no exception, along with the positive outcomes of the use of internet it has been witnessed in the society in the recent times, that there is a spurt in technology based crimes (Cyber-crimes) wherein the internet is used as a means to commit crime. It is an alarming fact that cyber-crimes have no territorial boundaries. The governments world over are grappling with this quintessential problem which is increasing by the day and have enacted laws to tackle the commission of cyber-crimes.

Cyber crimes

Cyber-crimes ranges from hacking of a website and accessing confidential information to stealing of intellectual property with the use of internet. It includes commission of criminal activities with the help of internet. The cyber-crimes have been generally classified into crimes against individuals, against property, against the administration (government) and against the society. Those against the individual include harassment through emails, cyber stalking, hacking, email spoofing, phishing, child pornography, defamation, hacking and dissemination of obscene materials and assault by threat. Those against property include intellectual property crimes, software piracy, cyber-squatting, cyber vandalism, transmitting virus, cyber trespass, salami attack, Trojan horse, data diddling and email account hacking. Those against the administration include cyber terrorism, cyber warfare, and possession and dissemination of unauthorised information. Those against the society include child pornography, cyber trafficking, online gambling, financial crimes and forgery.

Indian Cyber laws

India has enacted the Information Technology Act (IT Act) in the year 2000 with a primary objective of regulating the use and protection of technology for commercial purposes. It



specifies the punishments for the commission of cyber-crimes. It was amended in the year 2008 to combat the new exigencies of cyber-crimes. The original IT Act 2000 dealt with the legal recognition of electronic documents, digital signatures and the legal dispensation systems for cyber-crimes. Whereas, the amended Act of 2008 focused on data privacy, information security, defining practices to be followed by the corporates, redefining the role of intermediaries, recognising the role of Indian Computer Emergency Response Team, authorising an inspector to investigate cyber offences and it also included additional cyber-crimes like child pornography and cyber terrorism. The Information Technology Act has imposed criminal liabilities for the following offences:

- Tampering with Computer source documents¹-punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
- Hacking with Computer systems, Data alteration and other computer related Offences²-punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
- Punishment for sending offensive messages through communication service etc.³.-Imprisonment which may extend to three years and with fine.
- Punishment for dishonestly receiving stolen computer resource or communication device⁴- imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or both.
- Punishment for identity theft⁵- imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
- Punishment for cheating by personating by using computer resource⁶-imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.
- Punishment for violation of privacy⁷-imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both
- Punishment for cyber terrorism⁸-imprisonment which may extend to imprisonment for life.

¹Sec.65

²Sec.66

³Sec. 66A

⁴Sec. 66B

⁵Sec. 66C

⁶Sec. 66D

⁷Sec. 66E

⁸Sec. 66F



- Publishing obscene information¹-on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and on subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
- Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form²-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 on subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
- Punishment for child pornography ³ -Punishment for the first conviction is imprisonment for a maximum of five years and fine of ten lakh rupees and on subsequent conviction with imprisonment for seven years and fine of ten lakh rupees.
- Preservation and retention of information by intermediaries⁴- Non-compliance is an offence with a punishment of imprisonment up to three years or fine.
- Un-authorized access to protected system⁵
- Penalty for misrepresentation-⁶Punishment is imprisonment which may extend to two years or a fine of maximum of one lakh rupees or both.
- Breach of Confidentiality and Privacy⁷-Penalty for breach of confidentiality and privacy is punishable with imprisonment for a term up to two years or a fine of one lakh rupees or both.
- Publishing false digital signature certificates⁸-any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine of maximum of one lakh rupees, or both.
- Publication for fraudulent purposes⁹-imprisonment for a term which may extend to two years, or with fine of maximum one lakh rupees, or both.

In view of the increasing threat of terrorism in the country, section 69 now empowers the state to issue directions for interception or monitoring of decryption of any information

¹Sec.67

²Sec. 67A

³Sec. 67B

⁴Sec. 67C

⁵Sec.70

⁶Sec. 71

⁷Sec.72

⁸Sec.73

⁹Sec. 74



through any computer resource. Further, sections 69A and B, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect data or information through any computer resource for cyber security.

Indian Penal Code vis-à-vis Cyber Crimes

The increasing surge of cyber-crimes have necessitated the amendment of the Indian Penal Code (IPC) as well. The sections 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc. dealing with entry in a record which is false etc. have been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC the electronic records and documents on a par with physical records and documents with respect to commission of acts of forgery or falsification of physical records in a crime. The other cyber-crimes covered by IPC are sending threatening messages by email,¹ sending defamatory messages by email,² Forgery of electronic records,³ bogus websites⁴, cyber frauds⁵, e-mail spoofing⁶, web-Jacking⁷, e-Mail Abuse.⁸

Judicial Response

There have been a few trend setting judgements delivered that have set the pace of law governing cyber-crimes in India. Some of the cases quoted hereunder showcase the sensitivity of the judiciary to the gravity of cyber-crimes. There is an enormous onus on the judiciary to update their knowledge and hone their skills to curb cyber-crimes.

National Association of Software and Service Companies vs Ajay Sood & Others,⁹

In this milestone judgment in March 2005, the Delhi High Court declared 'phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages. Laying a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate entity to extract personal and confidential data from a customer. Though there was no specific legislation in India to penalise phishing at that point of time Delhi High Court held phishing to be an illegal act.

*Times Internet vs M/s Belize Domian Whois Service Ltd & Others*¹⁰

This case is an instance of cyber-squatting. The judgment reaffirmed the intellectual property of trademark passing off principle.

¹Sec 503 IPC

²Sec 499 IPC

³Sec 463 IPC

⁴Sec 420 IPC

⁵*ibid*

⁶Sec 463 IPC

⁷Sec. 383 IPC

⁸Sec. 500 IPC

⁹119 (2005) DLT 596, 2005 (30) PTC 437 Del

¹⁰CS(OS) No. 1289 of 2008 High Court of Delhi 10 November 2010



*RituKohli Case*¹

RituKohli Case, is demmed as India's first case of cyber stalking. It was a case of stalking by the former employee of the lady's husband. As the Indian cyber law was non-existent at the time of this case it was just registered as a minor offences under the Indian Penal Code.

*ArifAzim case*²

Also known as Sony- Sambhand.com case, this was India's first convicted cyber-crime case. IT was a case of misuse of credit cards numbers by a Call Centre employee. ArifAzim the accused was sentenced to probation for a period of one year as he had no previous criminal record.

*State of Tamilnaduvs Dr.L.Prakash*³

In this land mark case, a Fast track court in Chennai sentenced a surgeon Dr. Prakash to Life imprisonment in the year 2008. The accused was the first person to be arrested under the Information Technology Act. He was accused of sexually exploiting women and uploading their obscene pictures on the internet with the help of his brother based in the US. He was charged with offences punishable under Section 67 of the Information Technology Act, besides the provisions of the Indecent Representation of Women (Prohibition) Act, 1986 read with Section 27 of the Arms Act, 1959, and 120-B of the Indian Penal Code.

*State vsMohd. Afzal and Others*⁴ (Parliament AttackCase)

In this case of terrorist attack onParliament House Digital evidence played an important role during prosecution. The fake IDs used by the terrorists the entry pass sticker on the car used by them were all revealed by investigations to be all forged and made on the laptop seized from the terrorists.

*R vs. Whiteley*⁵

In this case the accused through unauthorized access to the Joint Academic Network (JANET) deleted, added files and changed the passwords to deny access to the authorized users. The accused was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers causing a loss of Rs 38,248. The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC and Section 66 of IT Act

¹ Farooq Ahmad: *Cyber Law of India (Law on Internet)*, 3rd Edn. New Era Law Publication, p-411

² V. Paranjape, *Cyber Crimes & Law*, Central law Agency, 2010, p-137

³ <http://timesofindia.indiatimes.com/city/chennai/Porn-doctor-acquitted-in-drugs-case/articleshow/6088338.cms?> last visited 30th October 2018

⁴ 2003 VIIAD Delhi 1, 107 (2003) DLT 385, 2003 (71) DRJ 178, 2003 (3) JCC 1669

⁵ (1997)20/11/1997



The State of Tamil Nadu vs. SuhasKatti¹

This case is the first conviction under section 67 of ITAct, it is a case of posting obscene, defamatory and annoying message about a divorcee woman by the accused who opened a n email account in the name of the victim. The accused was charged for the offences under section 469, 509 IPC and 67 of IT Act, 2000.

Conclusion

Taking into consideration the increasing proportions of cyber-crimes as revealed by the NCRB reports, there is an urgent need for education and awareness regarding the occurrence and commission of cyber-crimes. The Police and the judiciary at all levels have to be aware and sensitised to recognise and act fast to curb the growing trend of cyber-crimes in India. It is to be noted at this juncture that cyber-crimes are perpetuated by the criminals who are technocrats who understand the intricacies of information technology. This makes it all the more important for the judiciary and the law enforcing authorities to be updated on their knowledge of information technology and also expedite the cyber-crimes cases to ensure the accused are punished and the crimes are detected and controlled effectively. The cyber law is in place in India along with Indian Penal Code law of Evidence and Criminal Procedure, Banker's Book Act and the Negotiable Instruments Act to help the police and judiciary. To increase the rate of conviction the general public must be sensitised and made aware of the computer crimes and encouraged to report of illegal activities that they have fallen prey to. A proactive law enforcing agency and prompt conviction would definitely go a long way in helping to curb this growing menace.

¹4680 of 2004. Decided by the Chief Metropolitan Magistrate, Egmore, on November 5, 2004.



JUVENILE CYBERCRIMES AND SMARTPHONE-ADDICTION: A BRIEF REVIEW AND
PLAUSIBLE LAW REFORMS

Dr. Kubair

Rajiv Gandhi College of Law, Karnataka State Law University

&

Mr. Dhirendra V.,

I LL.B., Rajiv Gandhi College of Law, Karnataka State Law University

1. INTRODUCTION

Smartphones, for the purpose of the present discussion are cellular phones that have internet connectivity. According to the *statista*¹ the number of smartphone users in India since 2014 has increased from 21% to almost 36% in 2018. That is one in three people own a smartphone in India today. The number of smartphones sales in India in 2017 was around 30 million, which is comparable to the sales of two-wheelers in the same period. The number of smartphones and users in India is slated to increase and by a statistical projection, it is expected to reach almost 75 percent in two years, that is by 2020². The rapid increase in the smartphone usage is due to the policy change of the Government of India, which is pushing towards a cashless economy³ to bring in more transparency in the financial transactions. India is the second most populous country in the world, with smartphone users increasing to 60% by 2020 (*less than two more years*) and vehicular densities, has become more crime ridden as indicated by the National Crime Records Bureau (NCRB)⁴. Alarming, crimes against and by children have also commensurately increased⁵.

[†] 1st Year LL.B Karnataka State Law University, email: dv.kubair@gmail.com

¹ <https://www.statista.com/statistics/257048/smartphone-user-penetration-in-india/> (last accessed 1 November 2018)

² Sharma, 2017, Mobile phone penetration in India set to rise to 85-90% by 2020: report, *The Live Mint*, 17 May 2017, <https://www.livemint.com/Consumer/zxupEDYD560LJrnoRxcn4L/Mobile-phone-penetration-in-India-set-to-rise-to-8590-by-2.html> (last accessed 1 November 2018).

³ Agarwal and Arora, 2017, Here is Modi government's next big plan to make India a cash-mukt Bharat, *The Economic Times*, 1 September 2017, <https://economictimes.indiatimes.com/news/economy/policy/here-is-modi-governments-next-big-plan-to-make-india-cash-mukt-bharat/articleshow/60315980.cms> (last accessed 1 November 2018); Deepika, 2017, Digital India: Here's Modi's master plan to make Bharat a cashless economy, *One India*, 1 September 2017, <https://www.oneindia.com/india/digital-india-here-s-modi-s-master-plan-to-make-bharat-cashless-economy-2534295.html> (last accessed 1 November 2018)

⁴ <http://ncrb.gov.in/StatPublications/CII/ciimainpage.htm> (last accessed 1 November 2018)

⁵ Venugopal, 2016, More children fall prey to cyber crime as web users get younger, *The Hindu*, <https://www.thehindu.com/news/cities/chennai/more-children-fall-prey-to-cyber-crime-as-web-users-get-younger/article3509863.ece> (last accessed 1 November 2018).



The present brief review is aimed at understanding how the smartphones and connected devices have affected the children and how the existing statutes protect the children who suffer as victims and also are the perpetrators. Plausible reforms to the existing laws are proposed to alleviate the steep rise in the rates of juvenile cybercrimes and internet-addiction.

2. Nature of juvenile cybercrimes¹ and juvenile internet-addiction²

There are numerous crimes that are committed using cyber based technologies. The prominent ones that affect juveniles (between ages 5 to 18) are listed here:

- i. **Cyber Bullying**: A form of bullying or harassment using internet connected devices and smartphones³. Information Technology Act 2000⁴, §66A, which was struck down in March 2015.
- ii. **Hacking**⁵: To gain illegal access to a computer network, system, etc.
- iii. **Phishing**⁶: This a technique of extracting confidential information such as credit card numbers and username password by masquerading as a legitimate enterprise.
- iv. **Cyber stalking**: Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online.
- v. **Identity theft**⁷: Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name⁸.
- vi. **Child grooming**⁹: Befriending and establishing an emotional connection with a child on the internet to lower the child's inhibitions with the objective of sexual abuse detailed in ITA⁹.
- vii. **Child pornography**¹⁰: pornography that exploits children for sexual stimulation.

Apart from the crimes delineated above, there is another serious mental health issue, analogous to substance abuse (such as alcohol, intoxicating drugs) and occurs due to

¹ <https://en.wikipedia.org/wiki/Cybercrime> (last accessed 1 November 2018); Information Technology Act, 2000, Chapter XI, Offences, §65-78;

² https://en.wikipedia.org/wiki/Internet_addiction_disorder

³ Statista *supra* note 1.

⁴ Information Technology Act 2000

⁵ ITA 2000 *supra* note 202, Chapter XI, §66

⁶ ITA 2000 *supra* note 202, Chapter XI, §66A (struck down in March 2015), 66E

⁷ ITA 2000 *supra* note 202, Chapter XI, §66C

⁸ Federal Trade Commission, <https://www.consumer.ftc.gov/articles/0040-child-identity-theft> (last accessed 1 November 2018); "Aadhaar case", Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018.

⁹ ITA 2000 *supra* note 202, Chapter XI, §66D, 67B(c).

¹⁰ ITA 2000 *supra* note 202, Chapter XI, §67, 67A, 67B and 67C



excessive usage of internet connected devices, which has received a lot of attention by concerned parents and pediatric psychologists and is *internet-addiction*¹.

The cybercrimes pertaining to children in the list above can be classified into:

- a. children-children (CC): where both the perpetrators and victims are both children. The plausible crimes include: cyber bullying, cyber stalking, and child pornography, phishing; identity theft.
- b. children-public (CP): the perpetrators are children (or an individual child), while the victim is the public and not any particular individual, including organizations, Governments etc. The plausible crimes include: hacking, phishing and identity theft.
- c. children-adult (CA): where the perpetrators are children (or an individual child) and the victims are adults (or an individual adult). The plausible crimes include: hacking, phishing, cyber stalking and identity theft.
- d. adult-children (AC): the perpetrators are adults (individual or many) and the victims are children. The plausible crimes includes all those listed above, namely, cyber bullying, hacking, phishing, cyber stalking, identity theft, child grooming and child pornography.

Whenever cybercrimes are discussed, most believe it is usually the adult-children (AC) kind for which the laws are well codified² to handle the perpetrators. For example, when an adult commits a crime against a child, Chapter 9 of the JJA³ 2015 details the procedure and punishments for offences electronic or otherwise.

Juvenile cybercrimes in which perpetrators are children fall under CC, CP and CA are the latest ones and rising due to the ease of access to smartphones and internet connected devices. According to §89 of the JJA 2015⁴, entitled "*Offence committed by child under this Chapter*" reads

"Any child who commits any offence under this Chapter shall be considered as a child in conflict with law under this Act".

The Chapter 4: *Procedure in relation to children in conflict with law*, §10 to §26 JJA 2015⁵, discusses the procedure of handling juvenile offenders and punishments for offences by children. According

¹ Shaw and Black, 2008, Internet addiction: definition, assessment, epidemiology and clinical management, *CNS Drugs*, 22(5):353-65, <https://www.ncbi.nlm.nih.gov/pubmed/18399706> (last accessed 1 November 2018); Parasuraman *et al.*, 2017, Smartphone usage and increased risk of mobile phone addiction: A concurrent study, *Int J Pharm Investigation*, Jul-Sep; 7(3): 125-131. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5680647/> (last accessed 1 November 2018)

² ITA 2000 *supra* note 202.

³ Juvenile Justice (Care and Protection of Children) Act 2015.

⁴ JJA 2015 *supra* note 211, Chapter 9, §89.

⁵ JJA 2015 *supra* note 211, Chapter 4.



IPC 1860¹, children under seven years and between seven to twelve "*without sufficient maturity of understanding to judge of the nature and consequence of his conduct on that occasion*" are absolved of any crime committed. The recent amended JJA² considers minors of ages between sixteen and eighteen years as adults, when the committed crime is heinous in nature.

The cybercrimes committed by children could turn out to be serious and heinous with so many juvenile smartphones users. A brief review of several juvenile cybercrimes in the order of severity according to the existing statutes are discussed next.

3. Brief review of juvenile cybercrimes

According to the IPC 1860³ children below seven years are totally immune to any punishment of crimes, while children between the ages seven and twelve are liable depending on their circumstance. Above twelve years of age children can be tried under the JJA⁴. Children above twelve years are the ones who are commonly in high-school (eight standard onwards). Children who are sixteen and below eighteen are the ones in intermediate, pre-university, diploma in engineering, industrial training institutes (ITI). Children both in high-school and post-high-school are exposed to information technology as a part of their curriculum. There are instance of success stories⁵ of high-school children becoming millionaires by developing programs and apps for smartphones. The above success story clearly indicates the expertise gained by children at an young age. In corollary, this also indicates high-school children are capable and have committed several cybercrimes.

Post-high-school children who are undergoing technical education in diploma in engineering, industrial training institutes are definitely vulnerable to commit juvenile cybercrimes as they are professionally trained for maintaining computer servers, internet networks, and development of smartphone apps.

The smartphone and computer expertise gained by high-school and post-high-school level children described above could be used deviously, ending up committing juvenile cybercrimes listed as CC, CP and CA. It is important to note that, the author does not intend to portray that all children have a deviant attitude nor propose to prohibit children using advanced technologies. The intention is to make the world (especially the cyberspace and information

¹ Indian Penal Code 1860, §82 and §83.

² JJA 2015 *supra* note 211, Chapter 4, §15.

³ IPC 1860 *supra* note 214.

⁴ JJA *supra* note 211.

⁵ Borpuzari and Bhattacharya, 2016, India's youngest app developers Shravan & Sanjay Kumaran shows us how to hustle, *Economic Times*, 21 January 2016,

http://economictimes.indiatimes.com/articleshow/50668608.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last accessed 1 November 2018); Albert Costill, 2016, 25 kids that made \$1 million before graduating high school, *Due*, 9 December 2016, <https://due.com/blog/25-kids-made-1-million-graduating-high-school/> (last accessed 1 November 2018).



superhighway) a safe, enjoyable and nourishing place for everyone, including children, adults and the old.

3.1 Hacking

According to the definition under JJA 2015¹ any offence imprisonable for seven or more years is a *heinous offence*. According to ITA 2000², hacking or even trying to hack into a "*protected system*" (such as banking, e-trade, government, etc.) can lead to incarceration up to ten years and hence, can be classified as a heinous offence. The juvenile cybercrimes described under children-public (CP) mentioned earlier could become a heinous offence leading to very serious consequences to post-high-school children, if they were to commit such cyber-crimes. In a BBC report³ an ten year old child (Ms. Audrey Jones) was able to hack into the webpage that announced midterm election results in the state of Florida, USA within ten (10) minutes. Fortunately, the above hacking occurred on a *replica webpage* designed to test the hacking skills of children as a part of the "hacking for good" competition organized by r00tz Asylum⁴. The consequence of a child even attempting to replicate their hacking triumph on the real election webpage would be disastrous. In a 2016 report by Grimes⁵ in *info world* delineated eleven signs that a child might be into malicious hacking that parents should be watchful. Serious consequence do occur for children hackers as detailed in a report by Iyer⁶ on the cyber security platform TechWorm.

3.2 Child-pornography

According to ITA 2000⁷, transmission of obscene messages, pornography and child pornography can attract up to five years in prison for the first conviction. Transmission of obscene messages include sexting, threatening where explicit text messages in the form of short messaging service (SMS), or other electronic messaging services such as whatsapp, skype, google-chat might have been used. A thorough scientific study by Rice *et al.*, has reported on *sexting* by

¹ JJA 2015 *supra* note 211, Chapter 1, §2(33): "heinous offences", includes the offences for which the minimum punishment under the IPC or any other law for the time being in force is imprisonment for seven years or more.

² ITA 2000 *supra* note 202, Chapter XI: §70.

³ Dave Lee, 2018, Hacking the US mid-terms? It's child's play, *British Broadcasting Corporation*, 11 August 2018, <https://www.bbc.com/news/technology-45154903> (last accessed 1 November 2018);

⁴ <https://r00tz.org/> (last accessed 1 November 2018).

⁵ Grimes, Roger, A. 2016, 11 signs your kid is hacking -- and what to do about it, *Info World*, 5 July 2016, <https://www.infoworld.com/article/3088970/security/11-signs-your-kid-is-hacking-and-what-to-do-about-it.html?page=2> (last accessed 1 November 2018)

⁶ Iyer, Kavita, 2016, Here are world's greatest teenage hackers of all time, *Tech Worm*, 14 May 2016, <https://www.techworm.net/2016/05/5-ultimate-juvenile-hackers-time.html> (last accessed 1 November 2018).

⁷ ITA 2000 *supra* note 202, Chapter XI: §67, 67A and 67B.



children¹. Though the research findings was for the USA setting, it is very alarming and scaring that sexting amongst young children in the age bracket of twelve to fourteen is rapidly increasing. Although, no such research study has been conducted in the Indian context, there are several newspaper reports of sexting incidents by school children². Paul in the *The Daily Mail*³ report has explained the serious consequences of sexting of school-going children. The punishment for sexting is very harsh in the UK and could attract up to ten years in prison. As detailed in the report, even if the sexting was between children, it is still considered as a crime. Many a times, sexting between school-children might include willful exchange of their own nude pictures, which would become "child pornography" for both sending, receiving and distribution. Essentially, both the sender, who might be a school going girl and the receiver a school going boy, who are minors are considered offenders as in ITA 2005⁴ and POSCO 2012⁵. Under POSCO 2012, offenders of "child pornography" and possession thereof is punishable up to five and three years, respectively.

Another form of "child pornography" is being perpetrated, which is the posting of nude-selfies on webpages (such as facebook, instagram, snapchat etc.). Nude-selfies are selfies⁶, when a child photographs themselves in front of a mirror leading to the exposure of their private parts and are uploaded to the web by their own free-will without any coercion or undue influence. A report in Deccan Chronicle⁷ details the perils of preteens and teens faced by transmitting nude-selfies in

¹ Rice *et al.*, 2014, Sexting and Sexual Behavior Among Middle School Students, *Pediatrics*, 134(1), <http://pediatrics.aappublications.org/content/134/1/e21> (last accessed 1 November 2018)

² Hiranadani, 2016, It's time Indian parents tried to fill the generation gap with their children, *The Indian Express*, 23 June 2016, <https://indianexpress.com/article/blogs/cyber-bullying-its-time-indian-parents-tried-to-fill-the-generation-gap-with-their-children-2866893/>; Das Gupta, 2017, Sexting, cyberbullying by children may signal a criminal future: Govt manual, *Hindustan Times*, 25 May 2017, <https://www.hindustantimes.com/india-news/sexting-violence-and-cyberbullying-by-kids-may-signal-a-criminal-future-govt-manual/story-ZAZBWUIyoMKzLQNTunxVnM.html> (last accessed 1 November 2018); Sharma, 2018, Sexting among kids on the rise, time to educate parents, *Times of India*, 24 April 2018, http://timesofindia.indiatimes.com/articleshow/63886971.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last accessed 1 November 2018)

³ Paul, 2017, Why your child could go to prison for ten years for 'sexting' on their phone, *The Daily Mail*, 14 June 2017, <https://www.dailymail.co.uk/femail/article-4605090/Why-child-prison-sexting.html> (last accessed 1 November 2018)

⁴ ITA 2005 *supra* note, 203, §67B.

⁵ Protection of Children from Sexual Offences Act, 2012, Chapter III, §13, 14 and 15.

⁶ *selfie*: An image of oneself taken by oneself using a digital camera especially for posting on social networks, Merriam-Websters Lexicon.

⁷ Bhattathiripad, 2017, Internet no child's play, *Deccan Chronicle*, 18 March 2017, <https://www.deccanchronicle.com/technology/in-other-news/180317/internet-no-childs-play.html> (last accessed, 1 November 2018).



India. In the USA and UK, the consequences are very serious as detailed in many reports¹ and posting and transmitting nude-selfies are punished with imprisonment for up to ten years and the juvenile perpetrators are also listed in the registry of sexual offenders.

3.3 Cyberbullying

Bullying² that commonly occurs in schools, playgrounds is so stressful to children and can lead to depressions and mental health issues. School bullying includes, repeated teasing, badgering of a child by their classmates seniors and other children. Although no form of bullying should be tolerated or condoned, offline bullying has an effect of easing, as the act might be only limited to a particular geographical location (school, playground and such) and might automatically subside with time due to academic pressures in the schools. The added twist in the bullying is the *cyberbullying* and is rampant amongst school children in India. A research study conducted by Punjabi University in Patiala³ reported that a staggering 70% of students are victims of bullying (both offline and online) in India compared to other western countries. As detailed in the introduction, with the ease of access to smartphones and internet connected devices to school children the problem of cyberbullying has increased. The law in its present form does not cover cyberbullying by children and at best the ITA 2000⁴, whose §66A before being struck down in March 2015 had some mention of cyberbullying. The only recourse a juvenile victim might have is under *defamation* under the IPC⁵, which is not directly applicable to juvenile offenders. The important difference between bullying and cyberbullying, is that cyberbullying with the advent of technology does not stop and compounds due to the ease of access to the internet 24x7. The internet does not forget, once posted on the internet, any defaming and abusive comments stay there forever and is accessible from anywhere in the world. Without any deterrent the juvenile perpetrators feel emboldened and *raise the ante*. The ill-effects of

¹ Hasinoff, 2015, What to Do When Your Child Takes Nude Selfies, *Time*, 10 November 2015, <http://time.com/4105777/sexting-scandal-colorado/> (last accessed, 1 November 2018); Sexting boy's naked selfie recorded as crime by police, British Broadcasting Corporation, 3 September 2015, <https://www.bbc.com/news/uk-34136388> (last accessed, 1 November 2018); Teenage girl faces child pornography charges for sending explicit selfie over Snapchat, *Independent*, 24 December 2017, <https://www.independent.co.uk/news/world/americas/teenage-girl-14-explicit-picture-selfie-distributing-child-pornography-charges-police-rice-county-a8127001.html> (last accessed, 1 November 2018); Lohr, 2014, Virginia Teen Girl Accused Of Posting Nude Selfies, Arrested For Child Porn, *The Huffington Post*, 2 June 2014, https://www.huffingtonpost.in/entry/nude-teen-selfies-twitter_n_4737810 (last accessed, 1 November 2018).

² *Bullying*: abuse and mistreatment of someone vulnerable by someone stronger, more powerful, etc., Merriam-Websters Lexicon.

³ Blaya et al., Cyberviolence and Cyberbullying in Europe and India, *Cambridge University Press*, May 2018, <https://doi.org/10.1017/9781316987384.006> (last accessed 1 November 2018)

⁴ ITA *supra* note 202, §66A, was struck down on 24 March 2015 as it is in violation of Article 19(1) of Constitution of India

⁵ IPC *supra* note, 214, §499 *Defamation*, 500 *Punishment for defamation*.



cyberbullying on the victims has been reported¹ recently. The alarming conclusion of the above study is that cyberbullying victims are at a greater risk of self-harm and suicide. The obvious question in the view of the law will be, whether the juvenile cyberbullies are abettors to suicide of a child? If yes, then cyberbullying will turn out to become a most heinous crime according to IPC² and the consequences for the juvenile perpetrators will be grave as they might have to face death penalty or life in prison along with fine.

4. Internet- and smartphone-addiction

Addiction³ is a habit-forming use of a substance, in the context of internet- and smartphone-addiction, the substance is actually the internet or smartphones. Addiction due to substance abuse certainly is a conflict with the law. For example JJA⁴ §77 mentions about *psychotropic*⁵ substance. The dictionary meaning *psychotropic* is acting on the mind. The legal question is whether the *internet*, in the cases of excessive and abusive internet usage leading to internet-addiction can be considered as a *psychotropic* substance? Various medical and public health studies have been conducted in the Indian context to understand the above question⁶. The symptoms and addictive behavior does indicate a strong alteration of the mental state when internet is excessively used (or abused). Particular to the present discussion of juvenile smartphone- and internet-addiction studies in the Indian context have indicated an alarming trend of 39 to 44% addiction rates in adolescents⁷. With increase and ease in the smartphone

¹ John *et al.*, 2018, Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review, *Journal of Medical Internet Research*, 20(4): e129, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5934539/?report=classic> (last accessed 1 November 2018)

² IPC *supra* note, 214, §305, *Abetment of suicide of child or insane person*.

³ *Addiction*: compulsive need for and use of a habit-forming substance (such as heroin, nicotine, or alcohol) characterized by tolerance and by well-defined physiological symptoms upon withdrawal, Merriam-Websters Lexicon.

⁴ JJA 2015 *supra* note 211, §77.

⁵ *Psychotropic*: acting on the mind, Merriam-Websters Lexicon.

⁶ Krishnamurthi and Chetalapalli, 2015, Internet addiction: Prevalence and risk factors: A cross-sectional study among college students in Bengaluru, the Silicon Valley of India, *Indian Journal of Public Health*, 59(2), 115-121, <http://www.ijph.in/article.asp?issn=0019-557X;year=2015;volume=59;issue=2;spage=115;epage=121;aulast=Krishnamurthy> (last accessed 1 November 2018);

Sharma and Sharma, 2018, Internet addiction and psychological well-being among college students: A cross-sectional study from Central India, *Journal of Family Medicine and Health Care*, 7(1), 147-151, <http://www.jfmpc.com/article.asp?issn=2249-4863;year=2018;volume=7;issue=1;spage=147;epage=151;aulast=Sharma>, (last accessed 1 November 2018).

⁷ Goel *et al.*, 2013, A study on the prevalence of internet addiction and its association with psychopathology in Indian adolescents, *Indian J Psychiatry*. Apr-Jun; 55(2): 140-143. <http://www.indianjpsychiatry.org/article.asp?issn=0019-5545;year=2013;volume=55;issue=2;spage=140;epage=143;aulast=Goel> (last accessed 1 November 2018);

Davey and Davey, 2014, Assessment of Smartphone Addiction in Indian Adolescents: A Mixed Method Study by



availability in the future, this trend is certainly going to increase. A recent example of dangerous internet-addiction was the "*Blue Whale online game*"¹ challenge, which was so addictive last year (2017) and claimed more than hundred innocent lives. The Madras High Court took *suo motu* cognizance and rightfully banned the online game. Also the Supreme Court in a separate writ petition banned the game due to its dangerous addictive, self-harm and suicidal nature. Internet-addiction is not considered as a crime anywhere in the world, however, how can the law be amended to regulate and avoid adolescents from falling prey to internet- and smartphone-addiction is the question. Plausible law reforms and directions for reducing both juvenile cybercrimes and internet-addictions will be elucidated in the *Plausible amendments and recommended preventive measures* section next.

5. Plausible amendments and recommended preventive measures

There are two essential ingredients in order to commit a *cybercrime*, they are one, an internet connection (through internet service providers, data plans on smartphones) and two, an internet connected device (smartphones, tablets, laptops, smart-televisions, etc.). *Juvenile cybercrimes* can be committed only when children have access to both an internet connection and a connected device. Particular to the Indian context, smartphones, data plans and internet connections are expensive and can only be afforded by parents. As detailed in the introduction, parents feel that smartphones are beneficent for their children and give them unlimited access. Some parents might be lagging behind learning and updating the smartphone technology as compared to their children, leading to a *technological-generation-gap*. Unsupervised, unlimited access to smartphones is dangerous as detailed in the previous sections. Many studies, have taken an approach of educating the parents and counseling the children after a *juvenile cybercrime* is committed. An alternate and plausible method to educating parents is to *hold parents accountable* for the actions committed by their children using the internet connected devices they own. A motor vehicle can be used as an analogy, the MVA 1988² penalizes owners (say for example parents) who allows any person (their child) who is under aged or does not have a license to drive their motor vehicle. Another analogy is of road safety where parents teach their children how to safely use the roads and cross them. Similarly, internet is popularly called "*information superhighway*", and in order to navigate the *virtual-superhighway* the rules of the road should be followed, failing which leads to undesirable and longstanding consequences. Another plausible amendment would be the introduction of a law on the lines of JJA³, holding

Systematic-review and Meta-analysis Approach, *Indian Journal of Preventive Medicine*, v.5(12), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4336980/> (last accessed 1 November 2018)

¹ "Blue Whale online game case", The Registrar (Judicial) vs The Secretary To Government on 12 September 2017, Madras High Court; Kalita vs Union of India, 1 November 2017, Supreme Court;

² Motor Vehicles Act 1988, Chapter 2, §4, Chapter 13, §180.

³ JJA *supra* note 211, §77 "*Penalty for giving intoxicating liquor or narcotic drug or psychotropic substance to a child*".



parents liable if the child becomes an internet-addict. As the maxim goes, "*Ignorantia juris non excusat*", parents should not be permitted to claim excuse of not knowing the law. The main idea is not to punish loving-parents, but to protect their children from the perils of excessive and devious usage of smartphones.

There are health hazard notifications on computer keyboard and mice by their manufactures¹, which is mandated by the law. Such a notification should be imprinted on the packages of smartphones and also on the phones itself. The warning should at least indicate "*prolonged usage of smartphones could be addictive and should be used moderately. children should use only under the supervision of an adult*". The warning will act as a reminder to the juvenile users whenever the devices are used. The above idea is similar to the campaign against alcohol and cigarettes.

Most schools have computer literacy programs as a part of the curriculum during middle and high school (ages between 12 to 15). Curriculum of such computer classes/laboratories should impart internet safety education and lawful practices to be followed while using connected devices. Students found breaking rules in laboratory sessions can be detected, monitored and corrected before any escalation of the child's devious behavior.

Both the ITA 2000 and JJA 2015 in its current form needs to be amended to specifically include juvenile cybercrimes. These amended rules and regulations of ITA should be disseminated either as a separate course or a several chapters/units in regular courses, in Diploma, Industrial Training Institutes, pre-university courses for the benefit of the children in the post-school age group (between 16 and 18).

Most engineering students own laptop computers, smartphones and creatively explore the internet. They should be taught the rules of the internet-highway in order to navigate safely without getting into conflict with the law and also the consequences of breaking the law. At least one mandatory course in the first two semesters of undergraduate engineering degree classes for all streams detailing the ITA will be helpful.

6. Conclusions

Juvenile cybercrimes and internet-addictions are deviant behavior that are not defined under any of the prevailing laws of the land, including IPC, ITA or JJA. Concurrent amendments of the above Acts holding parents liable along with educating them can curb escalation of juvenile cybercrimes. Childhood pranks, which were let off as childish behavior before the internet existed, when done online becomes a serious crimes. A lenient view of some acceptable online childish behavior should be treated as childish and let off. Further monitoring and counseling is advised rather than punishing harshly. Post-high-school children, who are at the threshold of being adults (ages 16 to 18) need to be educated well by disseminating the ITA as part of their college curriculum. Amendments and suggestions discussed in the present review is hoped to lead to a safe, pleasant and productive internet surfing for children, parents and all *netizens* alike.

¹ "Some experts believe that the use of any keyboard may cause serious injury to your hands, wrists, arms, neck or back." is the warning imprinted on computer keyboards as mandated by the Law. https://www.logitech.com/images/pdf/roem/Logitech_Keyboard_Comfort_BPG2009.pdf (last accessed 1 November 2018),



EVOLVING CYBER LAW JURISPRUDENCE IN INDIA

P. Prasanna Kumar,

Assistant Professor, Sri Kengal Hanumanthaiya Law College.

prasna1976@gmail.com

INTRODUCTION

Bill Gates in his book "The Road Ahead", gives a mention about data protection in the chapter critical issues which states Loss of privacy is another major worry where the network is concerned. The potential problem is not the mere existence of information. it is the abuse that makes me worry.

QUOTE BY MICHEAL LEWIS THE DEFINITE SMELL INSIDE A SILICON VALLEY START UP WAS A CURRY. IN HIS BOOK "THE NEW THING; A SILICON VALLEY".

At the onset of the internet and technology a new phenomenon known as cyber law has emerged. Digital technology and new communication system have made dramatic changes in our lives. Technology is a double edged sword it can be used for good as well as bad purposes. people are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. information stored in electronic form is cheaper and it is easier to store ,retrieve and speedier to communicate. The United Nations Commissions on International Trade Law adopted the model law on electronic commerce in 1996 keeping in view the urgent need to bring suitable amendments in the existing law to facilitate commerce and with a view to facilitate electronic governance, The Information and technology Bill was introduced in the parliament and was passed on 17th October ,2000.The fundamental goal of cyber laws is to legalize human behavior and to have a statutory remedy in case of damage or copies data in the form of monetary damages not exceeding Rs one crore. These technology and its growth has been a challenge for the cyber law jurisprudence today and through out the world the courts are dealing with new challenges. The IT Act of 2000 seeks a remedy for most of the problems and it has also amended various other acts which are as follows; The Indian Penal Code,1860,the Indian Evidence Act,1872,The Bankers Book Evidence Act,1891,The Reserve Bank of INDIA act,1934.

INDIA is called the ransom ware capital of Asia as cyber threats are rising steeply. cyber crime is the crime of the future .It is much more easily committed and less easily identified, another important factor is that the laws are not kept in pace with the technology. It started with the invention of the computers and the pivotal role played by the computer has brought tremendous changes today.

Charles Babbage conceived that a machine which can perform calculations can be used to perform any task provided its design is such that its internal parts could be employed in different ways, so that when a particular task was being tackled a unique sequence of internal



activity would be set up, with each different task being tied to unique internal patterns of actions. All that was needed was a way to tell the machine which patterns of action were to be employed at any one point of time. Charles Babbage was well ahead of time .

Alan Turing worked in artificial intelligence and wrote a paper in 1936 on computable numbers, which described the concept of a machine called turing machine which could be adapted to any problem capable of human solution.

George Boole demonstrated that logic can be expressed in mathematical notations and gave us Boolean algebra or symbolic logic to the sphere Of Mathematics.

SCOPE

IT Act brings about an era of electronic governance which prescribes rules and regulations to maintain an electronic documents. with the amendment in the year 2008, sections 6A,7A,10A have been inserted to govern electronic governance

Section 6A empowers the Appropriate Government to authorize any service provider to upgrade, maintain, or perform other services through electronic means through retention of service charges.

Section 7A DEALS WITH AUDIT OF ELECTRONIC DOCUMENTS.

Section 10A accords legal sanction to the contracts entered electronically.

But due to the rapid increase in the internet which is border-less .one can do business from any part of the world and it has created certain conflict of laws which need to be resolved. There are some issues in case of defamation where difficulties arise if substantive law relating to a case is different at the place where it is hosted and where it is downloaded; it could be legal at the place of hosting and illegal where it is downloaded.

Yahoo case which involved display of nazi material and paraphernalia. The French filed a case against yahoo and got an order to destroy all nazi related messages, images and text stored on its server. But yahoo filed a case before the US district court for a declaration that French court orders were not enforceable in the US as it would violate the first Amendment of the US Constitution. The question involved in the yahoo case was a difficult one and the future hold the answer for such type of issues which was dismissed on certain grounds.

Cyber crime is a crime that involves a computer and a network which may be used in the commission of a crime or it may be a target. These types of crimes have become high profile and threatens a nations security.

The information technology act deals with the following kinds of cyber crimes along with others.

1.tampering with computer source document.

2.Hacking.It refers to an unauthorized intrusion into a computer who may alter system or security features to accomplish a goal that differs from the original purpose of the system.



3.Publishing information which is obscene which leads the mind to get misled where children get easy access to obscene material .section 67 of the IT Act punishes that person who publishes an obscene material in electronic form.

Accessing to protected system, Breach of confidentiality and privacy, Cyber crimes other than those mentioned under the IT ACT, Cyber stalking, Cyber squatting

Data diddling. It is also called false data entry. The unauthorized changing of data before or during their input to a computer system. examples forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements.

Cyber defamation. It involves defamation of a person through the virtual medium publishing defamatory material against another person through the internet.

Trojan attack. It serves as a back door in a computer system to allow an intruder to gain access to the system later.

Web jacking. The hacker gains access and control over the website of another. he may even change the information on the site. This may be done for fulfilling political objectives or for money. recently the site of information technology was hacked b the Pakistani hackers and some obscene matter was placed there in.

The IT Act has made a tremendous change by legally recognizing the electronic format. Indeed, the IT Act is a step forward. companies shall be entitled to carry out electronic commerce using the legal infrastructure provided by the IT Act. The corporate world will be now able to use digital signatures with legal sanction under the IT Act. statutory remedy is also available to the corporate if an one breaks into their system.

PROBLEM

There is no shield that cannot be pierced; no fort that cannot be breached; and no computer system that cannot be hacked. However, E-Commerce and Information Technology will lose their relevance unless computer systems are secure.

SOCIAL MALWARE; phishing is one of the biggest cyber security risk where fraudulent websites offer customer support and even mobile applications are entries for attackers through the remote connection to compromise user systems.

DISTRIBUTED DENIAL OF SERVICE ATTACKS;

DOS attack means preventing legitimate users of service from using that service. It generally occurs when a web server is flooded with requests for information overwhelming the system .Although such attacks do not normally compromise information security, they do cost time and money .This may happen to flooding of a network, or disrupting connections between the machines, or disrupting service to a specific system or person or preventing a particular individual from assessing a service or illegitimate use of resources. now this is covered in India under the amended provisions of the IT ACT, ie., section 66 of it act2000.

DDOS is evolving into smaller strikes that cause risk and data and risk.



RANSOMEWARE

Ransom ware the attackers expect corporations to be able to pay higher ransom, which hold users data to a ransom.

INSIDER THREAT

These are the most dangers types of network threat .insiders have the ability to cause most damage they gain access sing legitimate credentials for various reasons insiders can exploit network security in ways that are difficult to predict.

CLOUD ATTACKS

Cloud storage is used and SaaS Resources as this will shift to cloud attacks happen new technology will surface to secure data.

CAUSES OF CYBER CRIME

1. Easy to access. There is a possibility of breach due to the complex technology and the hackers an steal access codes retina images advanced voice recorders that can fool biometrics and easily access and bypass firewalls to get past many security systems.
2. Capacity to store data in a small space. this makes it a lot easier for the people to steal data from any other storage and use it for Own profit.
3. Complex .The computers run on operating systems which are programmed on millions of codes and as the human mind is imperfect so they can make mistakes at any stage. The cyber criminals take advantage of these loopholes.
4. Negligence. due to the negligent factor most of the computer system is not protected and it makes it easy for the hacker to get access to the files and other documents via computers.

Cyber crimes which use computer network or devices to advance other end which include fraud and theft Information warfare.

Phishing scams-It is a fraudulent way of getting confidential information. in phishing unsuspecting users receive official looking e-mails that attempt to fool them into disclosing online passwords, usernames and other personal information. victims are usually persuaded to click on a link that directs them to a doctored version of an organization website.

Spam -It is an unsolicited e-mail. They are a menace and they should have a provision to unsubscribe them or they may not be sent unless they are asked for. This is covered under section 66A(c) of IT act with punishment up to three years and different amounts of fine or both.

TEN COMMON CYBER ATTACKS

DOS DENIAL-OF -SERVICE ATTACKS

CYBER SQUATING-It is registering of websites with famous names in the hope of selling them at a profit. These practices are illegal and creates confusion and makes money by offering links to other commercial domains.



TYPO SQUATING. It is held to be illegal by a service provider www.nasdaq.com, a corruption of the New York stock exchanges nasdaq.com.

CYBER STALKING-Cyber stalking is a crime of annoying or watching somebody or following somebody over a long period in a way that is frightening. It refers to the use of internet, E-mail, or other electronic communication devices to stalk another person. In India by the 2008 amendment act, section 66A has been inserted as punishment for sending offensive messages through communication service.

SPIM-It is a junk or unwanted instant messages, which is covered under section 66A(b) of the IT Act.

NEED OF CYBER LAW

In the computer world, nothing is confidential. Everything can be found out till the information is permanently destroyed or overwritten. It is necessary that the information should be preserved. The IT Act makes provisions to preserve, protect and retain information.

The Information Technology Act, 2000 tries to secure by providing preventive measures, civil and criminal liabilities for the illegal action, appointment of the controller and grant of a license to a certifying authority to issue electronic signature certificates and lays down standards to be maintained under section 18 of the IT Act, 2000 and to maintain standards according to section 30 of IT Act, 2000.

Under section 29(I) of IT Act the controller or any person authorized by him can access any computer and data if he has reasonable cause to suspect contravention of the IT Act. But, now after 2008 amendment these powers are limited now as it has been entrusted to the central government or the state government or an officer authorized by them under section 69 of the IT Act.

Section 67(c) has been inserted into the IT Act which requires intermediary to preserve and retain such information for such duration as may be prescribed by the central Government. If an intermediary contravenes it, he will be liable to be punished for a term which may be extended to three years with fine.

The Government has framed rules titled the information technology procedure and safeguard for monitoring and collecting traffic data or information rules, 2009.

Section 70A and 70B have been inserted in the 2008 amendment act which empowers the central government to appoint any government as National Nodal Agency and Indian Computer Emergency Response Team to provide cyber security which also give directions to service providers and data centers intermediaries corporate persons to be liable for punishment if they do not comply.

The IT Act also provides punishment for the following acts like misrepresentation under section 71, breach of confidentiality and privacy of information section 72, publishing false electronic certificate section 73 and 74.



Section 43A and 72A deals with civil and criminal liabilities.

The Government of India has released fonts and software in a CD for technological development of Indian languages in June 2005, which contain terms and conditions for their use, software conditions.

Cyberspace are difficult to govern and regulate using conventional law.

Cyberspace has complete disrespect of jurisdictional boundaries. Because hacker from India could break in to a bank's electronic vault using a computer in a room and transfer millions of Rupees to another bank to another country all within minutes. The hacker just needs a laptop (or) a computer and a cell phone to hack in to the account.

Cyber space is a gigantic area of networking where every second, millions of e-mails, fax, and messages are being transferred around the world, even billions of transactions are being done in the world.

Cyberspace offers enormous potential for anonymity to the people. Information is readily available with encryption software and concealing tools that smoothly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

The law of real world cannot be interpreted in the emerging cyberspace to include all the aspects of the cyberspace.

However, substantial legal questions have been arisen in many contexts. The digital medium provides security or shields to the anonymity and fake identity profiles. In the recent survey made by the experts, it shows that there are numerous internet users receiving unsolicited emails which contain obscene languages and harassment. The cyber-stalking takes place to those people who put their individual profile information on the social media.

SOURCES AND DATA

The primary sources of cyber law in India is the Information Technology Act of 2000 (17 October 2000). IT (Amendment) Act, 2008 is known as the cyber law. The primary objective of the Act is to provide legal recognition to e-commerce and to facilitate filing of electronic records with the government. The IT Act also introduced various cyber-crimes and provides strict punishment and also fine.

The Information Technology Rules, 2000 also came into force. These rules state the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003 and 2006.

There are more than 57 laws that are amended in India. There are more than 27 offences (illegal acts) that include sexual abuse, violation of privacy, Cyber terrorism, Hacking with computer systems, Data Alteration, decryption of any information through any computer resource.



,unauthorized to protected system, publishing false digital certificates are punished under the Information and Technology act,2000.

Inventions and technologies widen the challenges in this world where it is a challenge to the jurisprudence in dealing with the business. the IT act seeks remedy to all the problems. the IT Act prescribes punishment for publishing obscene content in any electronic form under section 67,67A and 67B dealing with Indian morality and also section 292 of the IPC

DATA

The NCRB released its data relating to crime which states there is a 6% increase in the cybercrimes as compared to 2015. There are about 12,317 cybercrime cases in 2017 in India. But some cases are unreported. Uttar Pradesh is the highest with 2,639 cases reported.

OBJECTIVES

The amended information and technology act, 2000 should be amended to look into the matter of recent development in technology.

To guide and inspire people to know where to approach in case of doubt when using internet.

The websites should be monitored with affordable basic awareness and create a platform to seek appropriate remedy.

Privacy should be protected and it should not violate the information and misuse of personal data.

E commerce and suitable legislations should be passed to protect the customers safeguarding their personal information.

Awareness should be created by the government and people should be more conscious of it.

Login username password and other details with internet and computer systems should be secured and protected.

Effective software should be developed to solve the problems of cyber law.

DISADVANTAGES OF CYBER SECURITY

THE FIVE LAWS OF CYBER SECURITY

1. There is a vulnerability and will be exploited.
2. Everything is vulnerable in some way.
3. Human beings trust even when they shouldn't
4. With innovation comes opportunity for exploitation
5. When in doubt, refer law no 1

given by Forbes Technology Council, Atlanta, Boston

SUGGESTIONS

1. USE STRONG PASSWORDS. unless passwords are unique to each user and a secure password policy is enforced, it will be difficult to prove that a particular user has committed an illegal act.
2. Social media profiles less public



3. Secure your mobile devices
4. Protect your data
5. Protecting your identity online updating the computer with the latest software
6. Security software update
7. Calling the right person for help
8. Check and aware of data theft.

ISSUES

The GOLD CASE

Gold and Schifreen the accused were hackers who entered the data base of one prestel systems and were charged for forgery but were acquitted later .But the Law Commission in England recommended hacking to made penal.

DATA PROTECTION. Section 43A AND 72A HAVE BEEN INSERTED IN THE 2008 AMNDMENT ACT IN IT ACT.

It states that any person including an intermediary who has secured access to any material containing personal information in terms of lawful contract discloses the same with intent to cause or knowing he is likely to cause wrongful loss or wrong gain, then the offender is liable to be punished with imprisonment for a term which may extend to three years, or fine which may extend to five lakhs.

BAZEE.COM CASE-Bazee.com is a subsidiary of ebay and provides selling and buying of items. A pornographic video clip was put to sale on this site. According to the person in charge of Bazee.com it was without his knowledge. This may happen as it is almost impossible to supervise each item put on sale. This video clip was taken off immediately as soon as this information was given. nevertheless the person in charge was arrested and kept behind the bars.

A prima facie case was made under section 292(2)(a) and 292 (2)(d) of the Indian penal code,1860 against the petitioner in the Bazee.com case, but the petitioner stands discharged under these sections as the Indian Penal Code does not recognize the concept of an automatic criminal liability attaching to the director even when the company is accused, and the charge sheet nowhere implicates the petitioner in his individual capacity but implicates him as the managing director of the company.

But in case of software protection the Government should have released the terms and conditions under open source license, but except IIIT, Hyderabad which clearly states that the software can be used for personal use and cannot be used for any other purpose.

CONCLUSION

There should be a clear well defined law to tackle the onset of changing scenario in the cyber space. we need to be updated with new legislations to punish the criminals. Today in the present era we need a cyber jurisprudence based on cyber ethics which the growing problem of



cyber crimes. Though information technology act 2000 was passed to stop the ongoing menace in cyber space there are still certain matters which are unanswered under the present IT ACT 2000. There is a dire need to tackle the crisis as early as possible as the traditional criminal law principles are not sufficient to get the culprit red handed. since the cyber world has no boundaries it is the need of the hour to evolve new forthcoming legislations to cover each and every aspect of the cyber space. new laws have to be made to curb and punish the offender who are escaping in the high speed technological world. Inventions, discoveries and technologies widen scientific horizons but also pose new challenges for the legal world to solve problems and coming up with inconsistent answers and answer is IT Act which provides solutions to the problems which need to be made with new provisions to tackle cyber crimes in the future.

REFERENCES

Cyber laws by Justice Yatindra Singh

The making of micro; a history of the computers by Christopher Evans.

The chip by T.R Reid

The myth of the micro by Rodney dale and Ian Williamson

Cyber law and information technology by Talwanth

The road ahead by bill gates

NCRB reports on cyber crimes

R v/s gold, 1987 part 3 all ER page 680

www.ildc.gov.in

Yahoo case

Bazee.com case

WTO information technology agreement

WIPO

Govt India licenses

Arun Jaitely v/s Network Solutions Pvt., Ltd.

Amendments to Information Technology Act.

Indian Penal Code Section 292.

Roger Penrose – “The Emperors New Mind”



CYBER TERRORISM – A THREAT TO WORLD INFORMATION SECURITY AND

INTEGRITY: A CRITICAL STUDY

Mr. G. Senthil Kumar,

Assistant Professor, School of Law, VISTAS

&

Mr. Mohamed Zeejin

Assistant Professor, School of Law, VISTAS

Introduction:

After the Information Technological Revolution, World has been shrinking to a cyber-territory where it has brought everything under one roof. This gives both benefits and limitation of the information technology. Whistleblower who tries to bring the dark secrets of the government uses Information technology as a tool. At the same time, Cyber warfare and Cyber terrorism are the most serious threat to data integrity and information security of the world. The use of internet by the terrorist group and their supporters for the purpose of propaganda makes cyber terrorism wider. Apart from propaganda, the communication between terrorist groups, exchange of information and planning act of terrorism are done by the wide use of internet among the terrorist groups. This paper examines the cyber terrorism in the context of international aspect, legal and policy framework, investigation methods and prosecution.

With the rapid growth of Information technology, there is both boon and bane to the human society. Speed, information access and connectivity are considered as boon, at the same time hacking, misuse of information, data thefts are considered as its bane. In this modern era of information world, every data or information which is circulated on internet was not protected and safe. Due to this, many attacks have been take place on both physical and mental aspects of the individual in the society. The common term related to information technological terms are cyber-crimes, cyber-attack and cyber threat. Apart from these cyber-crimes, the dynamics of war and terrorism related issues are greatly impacted by the information technology. Today, there are terms such as Cyber-War and Cyber-Terrorism used consistently in International relation and issues which cause various harm to the human race in the society. Georgia conflict, Israel conflict, U.S. 9/11 attack and India's 26/11 attack were modern time issues which were greatly affected by Cyber terrorism.

In this context, it is important to understand the various dynamics and linkages towards cyber-terrorism and other areas of cyber-crimes related to terrorist activities. The basic understanding of Information technology is needed before knowing the core of Cyber-threats and warfare.



Definition of information technology:

The international foundation for IR or IF provided three major definition.

1. It is used for the study, understanding, planning, texting and computer relating system that exist for the purpose of data, information and knowledge processing
2. It is science and solution for all aspects of data, information, and knowledge processing for all aspects of computer and computer related system that exist for the purpose of management processing.
3. It is a technology required for the processing of data and other information. It can be defined as the application of computer. It is a set of non-human resources but the way in which these resources are organized into a system capable to perform tasks it includes all matters concerned with the furtherance of computer science and technology.¹

In the above definition, the term “Information” includes data, text, sound, voice codes, computer program software's or data base or micro film or computer generated micro film. The information technology includes all the aspects and this aspects has to be play in a particular platform and it is known as “Cyber-Space”.

Cyber space

The word cyber space was coined by William Gibson, lived in Bloomsburg, London. Cyber space was first used by Gibson for the time in his 1982 story BURNING CHROME and popularised in his 1984 novel NUEROMANCER.

Cyber space is a graphical representation of data abstracted from banks of every computer in the human system. The term **CYBER SPACE** comes from **CYBERNETICS** from Greek word **KYBERNWTES** which means pilot or rudder. It was introduced by Robert Weiner for his pioneering work.

Cyber space is the electronic medium of computer network in which online communication takes place. Cyber space is of the data stored in large network in a three dimensional through which a virtually user can move. The cyberspace is notional environment in which digitalised environment is communicated over computer networks

Cyber Criminals & Weapons in Cyber Space:

There are different categories of Cyber Criminal are around the world. They are as follows

1. Novice

- Limited computer and programmingskills
- Rely on toolkits to conduct theirattacks
- Looking for mediaattention.
- Can causeextensivedamagetosystemsincetheydon'tunderstandhowtheattacks works.

¹Darrell, K. B. (2007). Issues in Internet law: Society, technology, and the law. U.S.: Amber Book. Pg.no.34



2. Cyber-

punks

- Capable of writing their own software.
- Have an understanding of the system they are attacking.
- Many are engaged in credit card number theft and
- Have a tendency to brag about their exploits.

3. Internal

employees

or

a. Ex-employees

or

Disgruntled Employees.

- May be involved in technology related jobs.
- Aided by privileges they have or had been assigned as part of their job function
- Pose largest security problem.

b. Petty thieves

- Include employees, contractors, consultants.
- Computer literate.
- Optimistic: take advantage of poor internal security.
- Motivated by greed or necessity to pay of other habits such as drugs or gambling.

4. Coders

- Act as monitors to the newbies. Write the scripts and automated tools that other use.
- Motivated by a scene of power and prestige.
- Dangerous-have hidden agendas, use Trojan horses.

5. Old Guard hackers

- Appear to have no criminal intent.
- Alarming disrespect for personnel property.
- Appear to be interested in the intellectual endeavor.

6. Professional Criminals

- Specialize in corporate espionage.
- Guns for hire.
- Highly motivated, highly trained, have access to state of the art equipment.

7. Information warriors/Cyber-terrorists

- Increase in activity since the fall of many Eastern bloc intelligence agencies.
- Well-funded
- Mix political rhetoric with criminal activity.

8. Political Activist



- Possible emerging category.
- Engage in hacktivism.

Cyber weapons:

We face a multiple threats in cyber space. One such threat is that of code being embedded in firmware of computer is that of malicious code being embedded in firmware of computer or application software from foreign supplies. The bios is software that runs during the startup sequence where it configures devices and runs then boots the operating system.

Let's examine a few more of the top cyber threats.

1. Computer Virus Attacks(CVA)

A virus is a harmful software program that is secretly introduced into a system with the characteristic feature of being able to generate and distribute the computer system.

2. Distributed Denial of Service Attacks(DDoS)

DDoS attack is launched as many remote computer system as a hacker can compromise. When DDoS are launched, the attacks are hard to stop because the data flood originates from many computers from multiple locations.

3. Other Cyber weapons

There are a number of other types of software weapons. These other weapons include computer worms, software vulnerability, exploitation, info-blockades, root kits, botnets, key loggers logic bombs and sniffing, etc.

4. Direct Energy Weapons(DEWs)

The class of cyber weapon is capable of disabling enemy computer system computer system without the use of explosives. DEWs include high energy microwaves (HEWs), high power microwaves(HPWs), and transient electromagnetic devices (TEDs). This class of weapons operated by using pulses or beams of electromagnetic energy to disrupt.

Cyber Terrorism:

The FBI defined Cyber Terrorism, "the premeditated, politically motivated attack against information, computer system, computer programs and data which results in violence against non-combatant targets by sub national groups or clandestine agents".¹

One of the greatest threats to modern society in the 21st century is the threat of cyber-terrorism - acts of terrorism committed via the computer. As developed countries increasingly turn to computer networks to control their infrastructure, they also become increasingly exposed to the dangers of someone hacking into their systems. The range of cyber-terrorist acts can be extremely diverse - from hacking into the database of a medical center and deleting patients' information, to disrupting water and electricity supplies of an entire country, to

¹ The FBI is primary investigative agency of United States Department of Justice (DOJ), serving as both a federal criminal investigative body and a domestic intelligence agency. Available at <http://www.fbi.gov/quickfacts.htm> (Visited on Oct.29, 2018)



causing accidents by disrupting the transportation system. Experts in the field of cyber-terrorism believe it is no longer a question of whether this kind of attack will or will not take place, but rather a question of when and where cyber-terrorism will finally strike.¹

One of the essential differences between terrorism that strikes in a physical space and terrorism that strikes in cyberspace is logistical - it is exceedingly difficult to plan, coordinate, and execute a conventional terrorist attack, whereas cyberspace terrorism requires only the appropriate knowledge and a personal computer. Hackers can break into computer systems long-distance, without the need of any logistical support.

Terrorist groups have long noticed the opportunities cyberspace presents, and the internet's accessibility, anonymity and global character have made cyber-terrorism very attractive and difficult to battle. Today, most of the terrorist organizations' activity on the web focuses on propaganda, psychological warfare, the recruitment of funds and human resources, enemy surveillance and espionage, and coordinating activities. These actions are not yet considered terrorist acts, but they can contribute greatly to those advancing such acts.

Beyond hacking into systems and collecting information, which doesn't cause much damage on a national or international scale, there is also the possibility of more pernicious cyber-attacks. Although this stage has not yet been reached, the future threat of cyber-attacks is very plausible. Possible targets of such an attack are communications systems, banks, electricity, water, transportation, government services, emergency rescue services, and the systems responsible for storing and distributing natural gas and oil. Possible scenarios are hacking into the banking system, which could lead to a complete shutdown of a country's economy or a disruption of communications between airplanes and control towers, which could lead to serious loss of life and property.²

Less intimidating scenarios are the disruption of television and radio signals, traffic lights, student databases, etc. In fact, cyber-terrorism can potentially disrupt any part of our day-to-day lives, anytime and anywhere.

Cyber Terrorism in India:

In India, the issues of Cyber Terrorism come under the Purview of Cyber Crimes. There is no separate head for investigating the Cyber terrorism related cases. The cases of Cyber terrorism under cyber-crimes are enquired under three following heads:

- i) Offences registered under the Information Technology Act, 2000.
- ii) Offences under the IPC related to cyber crimes
- iii) Offences under the Special and Local Laws (SLL) related to cyber crimes

¹<https://en.idi.org.il/articles/17488>

²Kaur, G. (2012). Cyber terrorism and law: Cyber-crimes. Place of publication not identified: Lap Lambert Academic Publ.Pg.No 26



Crime Incidence: 12,317 cases of Cyber Crimes, which include crimes under IT Act (8613 cases), IPC crimes (3518 cases) and other SLL Crimes (186 cases), were reported in 2016. There was an increase of 6.3% in Cyber Crimes in 2016. While 11,592 cases were reported in 2015, the number has increased to 12,317 cases in 2016.¹ The below table analysis the cyber-crime trends

Table: 1 Analysis of Cyber-crime Incidence

SL	Crime heads under IT Act	Cases Registered				Persons Arrested			
		2013	2014	2015	% Var.	2013	2014	2015	% Var.
1	Tampering Computer Source Documents (Sec. 65 of IT Act)	137	89	88	-1.1	59	64	62	-3.1
2	Computer Related Offences (Sec. 66 to 66E of IT Act)	2,516	5,548	6,567	18.4	1,011	3,131	4,217	34.7
3	Cyber Terrorism (Sec. 66F of IT Act)	-	5	13	160.0	-	0	3	-

Source: NCRB.nic.in

In this table, we can infer that the cyber terrorism related provision will come under the Section 66 F of the Information Act, 2005. No other provisions are there to investigate the Cyber terrorism related cases.

Conclusion:

So far as India is concerned in order to combat cyber terrorism through law, the Information Technology (Amendment) Act, 2008 has been enacted to include the same within the meaning of offences and therefore, is made punishable. Though, cyber terrorism has not been defined, but sec. 66(f) of the Information Technology (Amendment) Act, 2008 prescribes as to when cyber terrorism is said to have been committed. The need of the hour is to improve the infrastructure facilities and upgrading the investigating tools for Cyber-Terrorism. To ensure the World Information Security Protection and investigate the Cyber- Terrorism related crimes there should be more participation from the various stakeholders such as Government, International Bodies, and Private computer companies.

REFERENCES

1. Darrell, K. B. (2007). Issues in Internet law: Society, technology, and the law. U.S.: Amber Book.

¹ <https://mha.gov.in/sites/default/files/MINISTRY%20OF%20HOME%20AFFAIR%20AR%202017-18%20FOR%20WEB.pdf> pg.60



2. Kumar, G. R. (2006). Cyber-crimes: A primer on internet threats and email abuses. New Delhi, India: Viva Books Private Limited.
3. Kaur, G. (2012). Cyber terrorism and law: Cyber-crimes. Place of publication not identified: Lap Lambert Academic Publ.
4. Samrao, C. S. (2013). Cyber crimes. New Delhi: Random Publications.
5. <http://ncrb.nic.in>
6. <https://mha.gov.in>
7. Hindu Frontline



CYBER CRIMES ON WOMEN AND CHILDREN- A STUDY

Dr. P. Neeraja,

Assistant Professor, Department of Women's Studies, Sri Padmavati Mahila
Visvavidyalayam, Tirupati, Andhra Pradesh.

&

Dr. G. Indira Priyadarsini,

Assistant Professor, Department of Law, Sri Padmavati Mahila Visvavidyalayam,
Tirupati, Andhra Pradesh.

*There is one universal truth, applicable to all countries, cultures and communities: violence
against women is never acceptable, never excusable, and never tolerable."*

General Ban Ki-moon (2008) UN Secretary

Introduction

In today's digital era, the Internet and ICT are rapidly creating new social digital spaces and transforming how individuals meet, communicate and interact, and by this more generally, reshape society as a whole. This development is especially critical for new generations of girls and boys, who are starting their lives extensively using new technologies to mediate in their relationships, affecting all aspects of their lives. Technology is moving "much faster" than the law, making it necessary to understand why cybercrime happens and who are the people behind it. 'Cyber crime' is not a defined term but a catch-all phrase attributable to any offence involving an internet device. Most of the cyber crimes are listed under the Information Technology Act (IT Act), 2000, which was amended in 2008.

Whether at home or on the streets or during war, violence against women and girls is a human rights violation. Millions of women and girls around the world are subjected to deliberate violence because of their gender. Violence against women and girls (VAWG) knows no boundaries, cutting across borders, race, culture and income groups, profoundly harming victims, people around them, and society as a whole. Cyber-VAWG is emerging as a global problem with serious implications for societies and economies around the world

Digital technologies offer significant developmental and educational benefits for children. They offer new spaces for learning, play, socialization and entertainment. Most importantly, ICT and social media can offer incredible opportunities for children's active participation and empowerment, via digital citizenship, and ultimately contribute to the wider efforts towards meeting child-focused development goals. At the same time it is a threat for child's development and education. However, the lack of digital literacy and online safety



measures mean that children are also exposed to the risk of online crimes, abuse and exploitation. However, to date cyber-crimes against children in India are under-reported and have received very little attention and are not included in the National Crime Records Bureau statistics as a separate category.

With this backdrop, this paper is an attempt to discuss upon various forms of cybercrimes that can be inflicted upon women and children and how they adversely affect their lives.

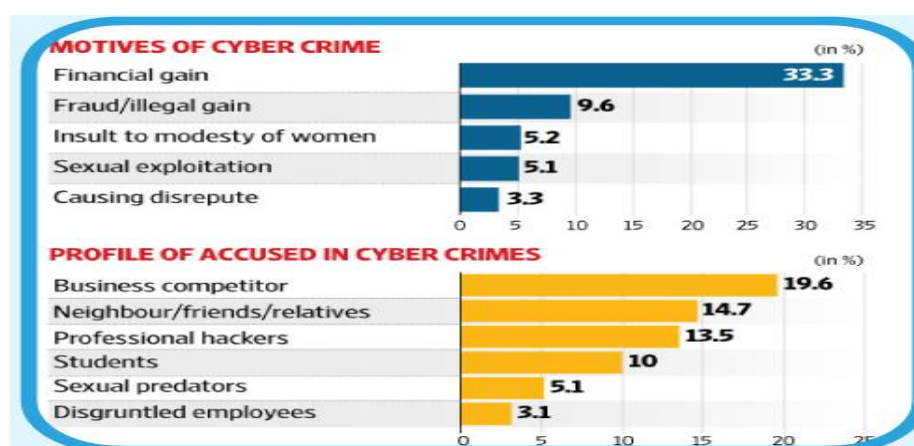
Cyber Crime Scenario in India

As per the NCRB data, there were about 12,317 cybercrime cases in 2016. This is a 6% rise as compared to 2015. Uttar Pradesh, with 2,639 cases reported the highest number of cases of cybercrime accounting for 21.4% of the total, followed by Maharashtra with 19.3% or 2,380 cases and Karnataka with 8.9% or 1,101 cases in 2016. However, experts say about 90% of cybercrime cases go unreported.¹

It is estimated that 35 per cent of women worldwide have experienced either physical and / or sexual intimate partner violence or sexual violence by a non-partner at some point in their lives. However, some national studies show that up to 70 per cent of women have experienced physical and/or sexual violence from an intimate partner in their lifetime. Women who have been physically or sexually abused by their partners are more than twice as likely to have an abortion, almost twice as likely to experience depression, and in some regions, 1.5 times more likely to acquire HIV, as compared to women who have not experienced partner violence.

About 27000+ cybercrimes reported in 2017 with an average of one every ten minutes. A huge number of these cases were addressed last year, but then almost the same number of cases lies un-addressed.

The types of cyber crimes that were reported



Source: National Crime Records Bureau, 2017

¹ “Cyber Crimes Against Women”. Available from: https://www.researchgate.net/publication/295381080_Cyber_Crimes_Against_Women.



Reasons for growth of Cyber Crimes against women

Most of our lives are public today on Social Media while most of the people free to share everything and expose their profiles to public instead of showing it to whom they connect with, most of the cyber crimes are either done by fraudsters or by someone who are known in the close circle. Various important reasons for growth of cyber crimes against women and children are:

- The transcendental nature of the internet- no boundaries, ever changing
- Low equipment cost
- Numerous vulnerable targets- Loneliness is a prime cause as many female students and staff live away from family and work for long hours over the computers. Thereby computers become their trusted pal.
- Easy concealment due to anonymity
- Most of the cyber crimes remain unreported due to the hesitation and shyness of the victim and her fear of defamation of family's name

Impact of cyber crime

Children and Women are more prone to cyber exploitation because the modesty, reputation and social standing of women are delicate. The same can be utilised to cause havoc in a woman's life. Cyber crimes bring tinges of tensions, disappointment, frustrations and unnecessary worries especially for women and girls. This is because of the negative use of digital and information technology; women and girls may be photographed inappropriately, touched inappropriately and may be photographed in such conditions, they may be stalked, their data may be unauthorised accessed and misused and over all, they may also be targeted for revenge porn. Being a victim of cyber crime could be most traumatic experience where her right to dignity, life, privacy will be infringed

Cyber offences against children are spreading and diversifying across India as new methods are used to harass abuse and exploit children. Cyber-crimes against children have many forms including sex-texting, online grooming, production and distribution of child harmful material, cyber bullying, etc. Girls and boys, including adolescents, are increasingly spending more time online and start using the Internet at younger ages than ever before. Although girls' and boys' access to information and communication technologies (ICTs) remains dominant in high-income countries, the rapid expansion of affordable, accessible Internet through mobile technologies in low- and middle-income countries is bringing more children to the Internet worldwide. No doubt ICTs bring tremendous benefits to children, providing access to information, education, entertainment and social networks that broaden their horizons and stimulate their creativity. But at the same time it can lead to harmful consequences and risks to their safety, personal development and well-being. While both girls and boys are vulnerable to



the different risks and harms related to the misuse of ICTs, girls have been disproportionately victimized in sexual abuse and exploitation through the production and distribution of child sexual abuse materials¹

Imperative in eliminating cyber VAWG

The first imperative in eliminating cyber VAWG is prevention. Changing social attitudes and norms is the first step to shifting the way online abuse is understood as a serious challenge. Violence is not new, but cyber violence is, and the public needs to recognize this and address it as a priority issue. Sensitization to cyber VAWG must include educating the next generation of ICT users, both boys and girls, through their parents, teachers and wider communities, as well as police authorities and the justice systems.

The second imperative is to put in place and implement safeguards to secure safe online spaces. Over the years, traditional VAW safety measures have evolved to include women's shelters, crisis centres, help lines and education. In light of the new cyber VAWG challenge, the digital world also urgently requires safety measures to keep up with a rapidly evolving Internet. This will necessarily require resources, attention and active participation of industry (digital gatekeepers), civil society and governments. Third in this multi-level approach to addressing cyber VAWG are sanctions, which address laws as well as the will and ability of the courts and legal systems to enforce compliance and punitive consequences for perpetrators. Establishing necessary laws is a starting goal; the next steps should ensure effective implementation. Sanctions however cannot on their own accord, define or set societal norms, or deter unlawful activity, or remedy injuries. The challenge requires a broad-based societal action, engaging all stakeholders. For this reason, while part of the solution, a mere legal reform agenda alone centered on perpetrators or abusers would be limited in both its reach and impact. Free speech is a fundamental right, and its preservation requires vigilance by everyone. Free speech online requires the vigilance particularly of those who use the Internet. Some suggest that the establishment of a Cyber Civil Rights Initiative (CCRI) through international collaboration is necessary to ensure a safe Internet. Others still stress that international human rights principles already provide the underpinning for a safe Internet, with the Human Rights Council's recognition that human rights apply offline as well as online.¹³ International and national laws and trans-national collaborative alliances are slowly evolving to address common global concerns of cyber VAWG, but if not dealt with commensurate to the challenge, crimes committed are likely to continue to increase, as more of the world goes online and these technologies become more and more a part of everyday life. Each of the above imperatives of sensitization, safeguards and sanctions supports the others, and will need consistent,

¹ National Dialogue on Gender-based Cyber Violence, https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Molly_Ghosh.pdf



collaborative action at many levels. Failure to address and solve cyber VAWG could significantly impede the digital inclusion of women everywhere, putting women at increasing disadvantage for being excluded from enjoying the benefits of ICTs and the Internet.

It is essential to have your privacy settings have to be set in such a way that individuals you are not connected don't get to see a lot of your personal information. Secondly, everything doesn't necessarily have to go on social media.

Legal provisions

Cyber crime is a global phenomenon. With the advent of technology, cyber crime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole. Even though India is one of the very few countries to enact IT Act 2000 to combat cyber crimes, issues regarding women still remain untouched in this Act.

Laws relating to cyber crimes against women are Indecent Representation of Women (Prohibition) Act, 1986 and the Information Technology Act, 2000. Of these the IT Act is not a gender-specific act but certain specific sections of the act deal with gender-specific crimes. The Indecent Representation of Women (Prohibition) Act, 1986 was enacted to prohibit indecent representation of women through advertisements or in publications, writing, painting, figures. Though it doesn't mention use of computers but as it applies to slide film and photograph also, it may ensure prohibition of indecent representation using internet.

The law and its officers are stuck in the 'physical', and the instinct in cases of violence is to focus on identifying physical injury. However, the logic of cyberspace is different from the real world, and hence, laws of the cyber world must be different from the real world. Most laws focus on punishment or protection but not prevention. However, it is 'prevention' that is the crux of state recognition of rights. When a woman makes a complaint of violence, it is a violation of her right that is being reported. And so the law must use language that forces officers of the law to acknowledge the inviolability of the right to dignity. Harm must be understood as an affront to dignity.¹

The IT Act 2000 was mainly to ensure legal recognition of e commerce within India. Due to this most provisions are mainly concerned with establishing digital certification processes within the country. Cyber crime as a term was not defined in the act. It only delved with few instances of computer related crime. Apart from conventional crimes under IPC, IT Act covers certain computer crimes against women. These acts as defined in Chapter XI of the Act are:²

¹ Justice Prabha Sridevan (retd.), Madras High Court, Chennai, speech on Gender-based cyber violence as real violence, National Dialogue on Gender-based Cyber Violence, TISS

² Soumik Chakraborty and Sreedhar Kusuman, Critical Appraisal Of Information Technology Act, Academiclike, <https://www.lawctopus.com/academike/critical-appraisal-information-technology-act-2000/>



1. Section 43- Illegal access, introduction of virus, denial of services, causing damage and manipulating computer accounts
2. Section 65- Tampering, destroying and concealing computer code
3. Section 66- Acts of hacking leading to wrongful loss or damage
4. Section 67- Acts related to publishing, transmission or causing Publication of obscene/lascivious in nature.

Punishment in section 65 and 66 is three years or fine up to two lakh rupees or both. For section 67 the first time offenders can be punished up to 5 years with fine up to one lakhs of rupees. Subsequent offence can lead to ten years of punishment and fine up to two lakhs of rupees.

In 2008 the Act has been amended included section 67A to 67C inserting penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form.

Forms of cyber crimes

The Cyber VAWG includes hate speech, hacking (intercepting private communications), identity theft, online stalking (criminal harassment) and uttering threats. It can entail convincing a target to end their lives (counselling suicide or advocating genocide). The Internet also facilitates other forms of violence against girls and women including trafficking and sex trade. Not only does commercialized sex on the Internet drive the demand for the sex industry overall, it also allows traffickers to use the legal aspects of commercial sex on the Internet as a cover for illegal activities. Some of the main uses of the Internet by traffickers include: advertising sex, soliciting victims on social media, exchanging money through online money transfer services, and organizing many of the logistical operations involved in transporting victims

The visibilization of gender has made anyone and everyone a 'feminist', and hence open to attack. However, the individualizing nature of the online space makes it difficult to fight back collectively. Part of the problem is that the structure of the Internet makes empathetic communities and the compromises that come with it unfashionable.¹

Cyber crimes are many, some of the most common type of Social Media Crimes are:²

Profile hacking: Profile hacking happens when, as a user, you are not able to log in to your account. Someone has complete control of your account and has changed all the credentials.

Photo morphing: Photo morphing is a special effect that allows a person to morph or change one image or shape into another without any difficulty.

¹ J.Devika, Centre for Development Studies, Trivandrum, speech on Women claiming the digital as 'own space': Reflections on the Malayalam public sphere, National Dialogue on Gender-based Cyber Violence, TISS

² Sorav Jain, C:\Users\ADMIN\Desktop\7 Types of Social Media Cybercrimes and How Women Should Deal With It.html,



Offer and Shopping Scams: You would often come across messages, post which would say 'Click on the link to claim the offer' or 'spin the wheel to win.' Women tend to fall for this scam on OLX, where the buyers try to give amazing offers.

Romance and Dating Scams: There are people out there who would connect to you on social media, interact with you, and persuade you to move to a different form of communication through various excuses. Once they realize that you are falling for them, they would send you small gifts to show you that it's same on either side. After a point the romantic period would start declining and they would start asking for monetary help in the form of recharge, booking flight tickets to meet and the list only grows

Link baiting: Link bait happens when the content of your website or pages gets linked to other sites because they want to and not because they have asked you.

Informational theft: Informational theft occurs when an imposter identifies key pieces of personally identifiable information like social security, driving license number in order to impersonate someone else. Businesswomen are also more likely to be at the risk of information theft especially with respect to her organization

Cyber bullying: Cyber harassment or online harassment is a holistic term which may include various types of harassments including cyber bullying. The term cyber bullying is defined as "abuse/ harassment by teasing or insulting, victims' body shape, intellect, family back ground, dress sense, mother tongue, place of origin, attitude, race, caste, class, name calling, using modern telecommunication networks such as mobile phones (SMS/MMS) and Internet (Chat rooms, emails, notice boards and groups)"¹.

Classification of cyber crimes: cyber crimes can be classified into three types

Crimes against person or Individuals: Harassment via email, Cyber Stalking, Dissemination of obscene Material , Defamation, Unauthorized control/access over computer system, Indecent exposure, Internet time theft , e-mail spoofing, Pornography including (Child pornography).

Crimes against Property: Computer vandalism, Virus transmission, Denial of service attacks, Unauthorized access over computer system, Intellectual property Crime, Financial scams and Frauds , Hacking, Sale of illegal articles.

Crimes against State/ Society: Intention to extract, Cyber terrorism, Distribution of private, Polluting youth through indecent exposure, illegal human trafficking online, online gambling

Conclusion

The biggest concern about the new Indian Cyber law relates to its implementation. The said Act does not lay down parameters for its implementation. Also when Internet penetration in India is extremely low and government and police officials, in general are not at all, computer

¹ K Jaishankar, Sexting: A new form of Victimless Crime?, International Journal of Cyber Criminology 3 (1), 21, 2009.



savvy, the new Indian Cyber law raises more questions than it answers them. It seems that the Parliament would be required to amend the IT Act, 2000.

All said and done, The Information Technology Act, 2000 is a great achievement and a remarkable step ahead in the right direction. The IT Act is a first step taken by the Government of India towards promoting the growth of electronic commerce so that Electronic Commerce in India can leap frog to success. Despite all its failings, it is a first historical step.

Women need to be more careful in using social media and should not be tempted to all fancy offers that are displayed. Children should be cautioned about the demerits and crimes that would be committed on computers. They should be made learnt about careful and vigilant use of social media. It's very difficult to remove the viral content on Social Media so it's always better to be safe than sorry

Recommendations

Policies and stricter laws should be made to discourage hacking activities among the youth and discourage victims from approaching hackers for removing offensive contents from the internet, mobile apps etc. ii. A woman centric information technology law must be drafted defining types of cyber crimes targeting women.

Existing provisions of Information Technology Act and IPC must be reframed and a constructive law should be made. Provisions from Indian Telegraph Act, 1885 must be included in the new law.

IT Act, 2000(as amended in 2008) is not women sensitive Act. It needs to be reviewed to introduce more innovative approaches in law.

The offences targeting online crimes against women must be made non-bailable and cognizable offences. The punishment terms must also be enhanced from simple imprisonment terms for 6 months/1 year, to minimum 3 years to maximum 5 years, or 7 years or more (in cases of grave offences). vi. Uniform identification numbers may be created for use to create accounts in the social media.

“Right to access the net”, “right to be forgotten” policies must be incorporated and such rights must be given the status of fundamental rights. viii. National commission for women should propose policies to include the issues of cyber crimes (especially crimes targeting women) in bilateral treaties. This would help in resolving cross-jurisdictional cases of cyber crimes targeting women.

National commission for women should propose to the government for framing stricter guidelines for intermediaries to pull down any content offensive to women.

As trans - Jurisdictional issues are involved in most of the cyber crimes, there is a need to develop a trans jurisdictional mechanism by signing bilateral treaties.

Under Section 357 A of CrPC, compensation is given to victims of crimes, who have suffered loss or injury as a result of the crime and who require rehabilitation. Compensation to



victims of cyber crimes on similar lines may also be considered as consequences of female victims of cyber crimes are equally devastating

More awareness programmes should be organized in schools and colleges in order to enable children and youth to learn about the dangerous consequences of misuse of information communication technology, existing and newly evolving varieties of cyber crimes targeting women and the general reasons for the growth of the issue, socio-legal ethics regarding photography in the public places (especially photography of women), to inculcate safe habits in the cyber space and to make them aware of legal rights and duties towards respecting right to privacy, right to life, liberty and child rights against abuses.

Cyber forensic labs in each district police head quarters should be set up. Over all, proactive policing for dealing with cases of cyber crimes against women is highly recommended.

Laws (such as Ss.292 and 294 IPC) and policies for restricting illegal and unauthorized selling of digital devices and porn contents by local shops should be strictly implemented. Women friendly mobile apps with a special chip or provision that can detect misuse of such apps in the name of helping women in distress may be developed.

References

World Health Organization, Department of Reproductive Health and Research, London School of Hygiene and Tropical Medicine, South African Medical Research Council (2013). *Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence*, p.2. For individual country information, see *The World's Women 2015, Trends and Statistics, Chapter 6, Violence against Women*, United Nations Department of Economic and Social Affairs, 2015 and UN Women *Global Database on Violence against Women*.

Facts and figures: Ending violence against women: <http://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures>

UNiTE Campaign Orange Day Action Plan: July 2017: Cyber Violence against Girls,
<http://www.un.org/en/women/endviolence/orangedayjuly2017.shtml>

<https://www.news18.com/news/india/ncrb-releases-data-on-cybercrime-rise-experts-fear-figures-do-not-reveal-real-picture-1597555.html>



CYBER CRIME AND PREVENTIVE MECHANISM- A CRITICAL ANALYSIS

Ms. Ramya Eswaran,

*Assistant Professor (On Contract), School of Excellence in Law,
The Tamil Nadu Dr. Ambedkar Law University, Perungudi, Chennai, Tamil Nadu*

1. Introduction

Cybercrime is an illegal activity conducted on a computer and it is evolving as a serious threat. A cyber-attack is an attack originated from a computer against a website, computer system or individual computer that compromises the confidentiality, integrity or availability of the computer or information stored on it. Cybercrime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet. Cybercrimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information in electronic form, e-mail bombing, etc. Historically, security measures have been applied to the protection of classified information from the threat of disclosure in a national security context. Recently much attention has been directed to the issue of individual privacy as it relates to personal information stored in computerised data systems.

2. Cybercrime

The present scenario of cyber crimes is summed up in the words "Amidst the surging excitement and internet, however, runs a deep thread of ambivalence toward connecting to the Internet. The Internet's evil twin is the home of "Bad Guys" hackers, crackers, snackers, stalkers, phone preaks and other creepy web crawlers, business fear that the Infobahn could suddenly veer into the highway to Hell"¹. Cybercrimes can be every bit as harmful to society as traditional crimes in the physical world. Cybercrime describes criminal activities committed through the use of electronic communications media, with regard to cyber fraud and identity theft through such methods as phishing, spoofing etc. According to tenth United Nations congress on "prevention of crime and treatment of offenders", the cybercrime can be categorized into two types.

(a) Cybercrime in a narrow sense (computer crime)

Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

(b) Cybercrime in a broader sense (computer-related crime)

¹Dr. FAROOQ AHMAD, CYBER LAW IN INDIA (LAW ON INTERNET), 306 (4th ed.2011).



Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network¹.

3. Classification of Cybercrimes

Cyber crimes can be classified on the basis of nature and purpose of the offence and have broadly grouped into three categories depending upon the target of the crime.

3.1. Cybercrimes against persons

The cybercrimes against person include crimes like hate messages, stalking, defamation and transmission of pornographic material. Such as:

3.1.1. Harassment via E-Mails

Harassment may be through sending letters, attachments of files & folders through e-mails. Harassment through social networking sites such as Facebook, Twitter etc. are increasing day by day.

3.1.2. Cyber stalking

It causes physical threat through the use of internet, email, text messages, webcam, websites or videos.

3.1.3. Hacking

Hacking is unauthorised control/access over computer system. It completely destroys the whole data as well as computer programmes. Hackers usually hack telecommunications and mobile network.

3.1.4. Cracking

This is one of the gravest cybercrimes. This involves breaking into others' computer system without knowledge and consent of the account holder and tampering with precious confidential data and information.

3.1.5. E-mail spoofing

E-mail spoofing is an act where the spoofed e-mail misrepresents its origin and shows its origin to be different from which it actually originates.

3.1.6. Child pornography

It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

3.1.7. Spamming

Spamming is sending of mass copies of unsolicited mails. There are mainly two methods used when spamming: newsgroup postings and email messaging, known as spam. An example of

¹Vineet Kandpal, Latest Face of Cybercrime and Its Prevention in India, *IJSBAR Sciences Vol. 2, No. 4, 2013. Pp. 150-156*



spamming would be sending out mass email to people who never requested it, as a chain letter or pyramid schemes.

3.2. Cybercrimes against person's property

It may be against property, the cybercrimes against property include unauthorised computer trespass, vandalism, and harmful programmes and unauthorised possession of computerised information. It can be classified as follows.

3.2.1. Intellectual Property Crimes

Intellectual Property consists of a bundle of rights. An unlawful act which deprives the rights of owner either completely or partially is an offence. The offences which violate the IPR of an individual include software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

3.2.2. Cyber Squatting

It is registering, trafficking in, or using a domain name with bad intent to profit from the goodwill of a trademark belonging to someone else. The cyber squatter offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price. For example, two similar names such as www.yahoo.com and www.yaahoo.com.

3.2.3. Cyber Vandalism

Vandalism is an act of intentionally destroying or damaging property of another.

3.2.4. Transmitting Virus

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it.

3.2.5. Cyber Trespass

It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

3.3. Cybercrimes against government

It may be against government. There are certain offences done by a group of persons intending to threaten the international governments by using internet facilities. They include,

3.3.1. Cyber Terrorism

Cyber Terrorism is a major burning issue in the domestic as well as global arenas. The common form of these terrorist attack on the internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

3.3.2. Distribution of pirated software

It involves the distribution of pirated software from one computer to another intending to destroy the data and official records of the government.



4. Convention on cybercrime

The Budapest Convention on cybercrime was opened for signature at Budapest (Hungary) on 23rd November 2001 and it entered into force on 1st July 2004. It was the first ever international treaty on Criminal offences committed against or with the help of computer networks such as the internet. The convention deals in particular with offences related to infringement of copyright, computer related fraud, child pornography and offences connected with network security. Its main objective is to pursue a common criminal policy aimed at the protection of society against cyber-crime, especially by adopting appropriate legislation and international cooperation¹.

5. Cyber offences control mechanism under Information Technology Act, 2000 and other laws

In order to prevent the various crimes in cyberspace, India adopted and placed the Information Technology Act 2000. It was the first step towards controlling and curb in cybercrimes. The Act contains the rules to prevent and control cybercrimes to regulate superhighway, to protect data and cyber world from any wrongful act or damage.

The Act, after amendments in 2008, appears to be more equipped to tackle cybercrimes. It has come to define several cyber acts as offences and prescribe punishments therefore. Relevant sections of IPC too have been amended in order to ensure that the cyber offences are covered by the wider definitions of crimes as also broader meanings to the keywords related to the world of crime.

The Act provides for appointment of an adjudicating officer who may decide cases and award compensation up to ten lakh rupees; and cases meriting a higher compensation shall be heard by a tribunal. The Act has renamed the tribunal and its head; and more clearly defined its procedure. The Cyber Appellate Tribunal is working to hear and decide appeals. By the end of 2011 it has disposed of about a dozen appeals filed before it, even as several others are being heard by it².

5.1. Penalty for damage to computer system

As per section 43 of IT ACT, 2000 whoever destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine up to 1 crore to the person so affected by way of remedy. According to section 43A which is inserted by IT Amendment ACT, 2008 where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data then a body corporate shall be liable to pay compensation to any person so

¹DR.S.R. MYNENI, INFORMATION TECHNOLOGY LAW (CYBER LAWS) 520-523 (1st ed. 2014).

²Dr. J.P. MISHRA, AN INTRODUCTION TO CYBER LAW 177-178 (2nd ed. 2014).



affected. Section 66 deals with hacking with computer system and provides for imprisonment up to 3 years or fine, which may extend up to 5 years or both¹.

5.2. Punishment under Information Technology Act, 2000 and Amendment Act, 2008

Sec. 66B provides Punishment for dishonestly receiving stolen computer resource or communicate on device.

Sec. 66C impose Punishment for identity theft.

Sec. 66D impose Punishment for cheating by personation by using computer resource.

Sec. 66E impose Punishment for violation of privacy.

Sec. 66F impose Punishment for cyber terrorism.

Sec. 67 of the Act prohibits online pornography and it is a punishable offence.

Sec. 72 of the Act impose penalty for breach of confidentiality and privacy.

Sec. 72A says Punishment for disclosure of information in breach of lawful contract.

5.3. Case law regarding cyber crime

In the state of Tamil Nadu vs. Suhas Katti 2004 can be considered as a landmark case in the history of cybercrime management in India. This was the first case in India wherein the offender was convicted under sec. 67 of IT ACT 2000 of India

In the case of Nascom vs. Ajay Sood 2005 and others is another landmark judgement delivered in March 2005, in which the Delhi High Court declared Phishing on the internet to be an illegal act. Though there is no specific legislation in India to penalise phishing, the court defined it under Indian Law as a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the customer but even to the person whose name, identity or password is misused. New multimedia and technology have become part of our daily lives in contemporary society and has made our life easier, quicker and cheaper in many ways. Such tremendous utility of information technology encourages the terrorists and other deviants in the society to sometimes use it as a tool or target to achieve their wrongful ends. This is not only a national issue of concern but a global one. Hence regulations must be made stringent to combat it.

In the case of Julian Assange vs. Swedish Prosecution Authority 2012 UKSC 22 is a good example of hacking. Julian Paul Assange is an editor, activist, publisher and journalist. He is the editor-in-chief and founder of WikiLeaks, which publishes submissions of secret information, news leaks and classified media from anonymous news sources and whistle-blowers. He was a hacker as a teenager, then a computer programmer before becoming known for his work with WikiLeaks. WikiLeaks became internationally well known in 2010 when it began to publish U.S. military and diplomatic documents with assistance from its partners in the news media. Bradley Manning has since been arrested on suspicion of supplying the cables to WikiLeaks. U.S. Air Force

¹T.V.R. SATYA PRASAD, LAW RELATING TO INFORMATION TECHNOLOGY (CYBER LAWS) 92-104 (1st ed. 2001).



documents reportedly state that military personnel who make contact with WikiLeaks or WikiLeaks supporters are at risk of being charged with communicating with the enemy, and the United States Department of justice reportedly has considered prosecuting Assange for several offences. During the trial of Manning prosecutors presented evidence that they claim reveals that Manning and Assange collaborated to steal and publish U.S. military and diplomatic documents. Since November 2010, Assange has been subject to a European Arrest Warrant, Assange has failed to surrender to his bail and has been treated by the UK authorities as having absconded. Since 19th June 2012, he has been inside the Ecuadorian embassy in London, where he has been granted diplomatic asylum. The British government intends to extradite Assange to Sweden under that arrest warrant once he leaves the embassy. It may leads to his extradition to the United States to face charges over the diplomatic cables case.

5.4.Cyber Offences Punishable under IPC

The 'mens rea' in case of cybercrime comprises of two elements. Firstly, intent to secure access to any programme or data held in any computer, computer system or computer network. Secondly, the person must know at that time that he commits the 'actus reus' that the access he intends to secure is unauthorised. The intent does not have to be directed at any particular programme or data held in any computer, computer system or computer network¹.

It is essential to have the knowledge of IPC, 1860 and Criminal Procedure Code, 1973 for better understanding of cyber offences. These Acts also offences specifically with providing punishments whereas the Criminal Procedure Code is procedure is procedural law and provides machinery for the punishment of the offenders against the substantive law. The first schedule of the Code of Criminal Procedure, 1973 provides the classification of offences. IPC was amended by infusing the term electronic. These all the electronic documents and records were made commensurate with the physical documents and records covered within the ambit of the IPC. The cyber offences were made punishable under IPC²:

Section. 292 IPC: Obscenity

Section. 292A IPC: Printing etc. of grossly indecent or scurrilous matter or matter intended to blackmail

Section. 293 IPC: Sale, etc., of obscene objects to young person

Section. 294 IPC: obscene acts and songs

Section. 420 IPC: Bogus websites, cyber frauds

Section. 463 IPC: E-mail spoofing

Section. 464 IPC: Making a false document

Section. 468 IPC: Forgery for purpose of cheating

Section. 469 IPC: Forgery for purpose of harming reputation

¹NANDAN KAMATH, LAW RELATING TO COMPUTERS INTERNET & E- COMMERCE 210-213 (5h ed. 2015).

²JUSTICE YATINDRA SINGH, CYBER LAWS 20-33 (5h ed.2012).



Section. 499 IPC Sending defamatory messages by e-mail

Section. 500 IPC: E-mail abuse

Section. 503 IPC: Sending threatening messages by e-mail

Section. 506 IPC: Punishment for criminal intimidation

Section. 507 IPC: Criminal intimidation by an anonymous communication

Also, some changes have been made to Evidence Act and a few other Acts to make them more in tune with IT Act.

6.Prevention of cyber crimes

6.1.Indian Computer Emergency Response Team

According to Section 70B of the Information Technology Act, 2000 the IT ACT the Central Government shall appoint this team to serve as the national agency for performing functions in the area of cyber security. They include, (a) Collection, analysis& dissemination of information on cyber incidents, (b) Forecast and alerts of cyber security incidents, (c) Emergency measures for handling cyber security incidents, (d) Coordination of cyber incidents response activities, (e) Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, preventative, response and reporting of cyber incidents and (f) Such other functions relating to cyber security as may be prescribed¹.

6.2. Power of the Central Government & State government to make rules

Section 87 & 90 of the Information Technology Act, 2000 Act has given general rule making powers to the central government and state government to give effect to the provisions of the Act, in exercise whereof the government has come out with a number of rules aimed at regulating the behaviour of intermediaries, to set guidelines for interception of information or blocking of websites for security reasons, etc.

6.3. Cyber Crime Cells in India

To solve cybercrime cases, Indian police developed cyber-crime investigation cells all over India. These Cyber Crime cell investigates in respect of cases pertaining to hacking, spread of virus, pornography, manipulation of accounts, alteration of data, software piracy, creation of false Web sites, printing of counterfeit currency, forged visas, theft of intellectual property, email spamming, denial of access, password theft, crimes with cell phones and palmtops, cyber terrorism etc.

6.4. Preventive Mechanism

6.4.1. Firewall

Computer users must use a firewall to protect their computer from hackers. Most security software comes with a firewall. Turn on the firewall that comes with their router as well.

6.4.2. Anti-virus

¹PAVAN DUGGAL, TEXT BOOK ON CYBER LAW 13-139 (2d ed. 2016).



Computer users are recommended to purchase and install anti-virus software such as McAfee or Norton Anti-Virus. Always use latest and updated Antivirus software to guard against virus attacks. To prevent loss of data due to virus attacks, always keep back up of your data.

6.4.3. Secure websites

It is advised by cyber experts that users must shop only at secure websites. Website owners should watch traffic and check any irregularity on the site. Putting host based intrusion detection devices on servers will serve the purpose. They should never give their credit card information to a website that looks suspicious or to strangers. Never disclose regarding personal information publicly on websites. This is as good as disclosing your identity to strangers in public place.

6.4.4. Passwords

Users must develop strong passwords on their accounts that are difficult to guess. Include both letters and numerals in their passwords. They must continuously update passwords and login details. By changing login details, at least once or twice a month, there are less chances of being a target of cybercrime. Never enter your credit card number to any site that is not secured, to prevent its misuse.

6.4.5. Monitor

It is suggested to monitor children and how they use the Internet. Install parental control software to limit where they can surf. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

6.4.6. Social network

Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs. Make sure that social networking profiles such as Facebook, Twitter, YouTube and MSN are set to private. Check their security settings and be careful what information users post online. Once it is on the Internet, it is extremely difficult to remove.

6.4.7. Secure mobile devices

More often than not, people leave their mobile devices unattended. By activating the built-in security features, they can avoid any access to personal details. Never store passwords, pin numbers and even own address on any mobile device.

6.4.8. Encryption

Protect Data to avoid criminals to hack. Use encryption for most sensitive files such as tax returns or financial records, make regular back-ups of all important data, and store it in a different location.

6.4.9. To Alert



Users must be alert while using public Wi-Fi Hotspots. While these access points are convenient, they are far from secure. Avoid conducting financial or corporate transactions on these networks.

6.4.10. Protect e-identity

Users must be careful when giving out personal information such as name, address, phone number or financial information on the Internet. Make sure that websites are secure.

6.4.11. Avoid being scammed

It is suggested that users must assess and think before they click on a link or file of unknown origin. Do not open any emails in inbox. Check the source of the message. If there is a doubt, verify the source. Never reply to emails that ask them to verify information or confirm their user ID or password.

7. Conclusion

In the 1990s, hacking was done basically to get more information about the systems. Cybercrime first started with hackers trying to break into computer networks. Some did it just for the thrill of accessing high-level security networks, but others sought to gain sensitive, classified material. Eventually, criminals started to infect computer systems with computer viruses, which led to breakdowns on personal and business computers. Many efforts are being taken at international level to curb cross border cyber threats. Indian police has started special cyber cells across the country and have started educating the peoples so that they gain knowledge and protect themselves from such crime. However, it is not possible to eliminate cybercrime from the cyber space. The only possible step is to make people aware of their rights and duties and to protect ourselves so that crime has no effect on us.



PREVENTION OF CYBER CRIMES IN INDIA- AN OVERVIEW

Dr. S. Madhuri Paradesi,

Associate Professor, Department of Law, Sri Padmavathi Mahila VisvaVidyalayam, Tirupati,
Andhra Pradesh

Introduction:

Cyber crime, or **computer-oriented crime**, is crime that involves a computer.¹ The computer may be employed in the commission of a crime, or it may be the target.² Cyber crimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".³

Cyber crime may pose a threat to a person or a nation's security and financial health.⁴ Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sex tortion, child pornography and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cyber crime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones". Internationally, both governmental and non-state actors engage in cyber crimes, including espionage, financial theft, and other cross-border crimes. Approximately \$1.5 billion was lost in 2012 to online credit and debit card fraud in the US.⁵ Cyber crimes crossing international borders and involving the actions of at least one nation-state is sometimes referred to as *cyber warfare*.

The emergence of the World Wide Web, smart-phones, and computers has transformed the world and enabled individuals to engage in crimes in a multitude of new ways. Cyber crime is becoming ever more serious. There is an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age. As the Internet becomes a part of our daily lives, criminals are increasingly using it to conduct cyber crime.

1. **Basic Definition of Cyber Crime:**

Cyber crime denotes illegal computer-mediated activities that often take place in the global electronic networks. The term has been variously defined by several authors. *Parker* considers it as 'encompassing any abuse and misuse of information that entails using knowledge of information systems'. *Philippsohn* views cyber crime as 'criminal activities conducted through



the internet'. *Thomas and Loader* define cyber crime as, 'illegal computer-mediated activities which can be conducted through global electronic networks'. *Richards* views it as, 'The illegitimate use of computer to conduct criminal activities'. Whereas, *Power* defines it as, 'The intentional access of a computer without authorization or by exceeding authorization and thereby obtain information to which the person is not entitled'.

Cyber crime describes criminal activities committed through the use of electronic communications media, with regard to cyber-fraud and identity theft through such methods as phishing, spoofing, etc. There are also many other forms of criminal behaviour through the use of information technology, such as harassment, defamation, pornography, cyber-terrorism, industrial espionage and some regulatory offences.

2. Categories of Cyber Crime:

Against Individual:

This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming".

Against Property:

Offenders stoop to stealing and robbing even in the cyber world. In this case, they can steal a person's bank details and drain off money; misuse credit-card to make frequent purchases online; run a scam to get naive people to part with their hard-earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

Against Government:

Crimes against a government are referred to as cyber-terrorism. If criminals are successful, it can cause devastation and panic amongst the citizen. In this class, criminals hack government websites, military websites or circulate propaganda. The committers can be terrorist outfits or unfriendly governments of other nations.

Against Organisations:

Organisational cyber crime is all too common and growing in large proportions in today's world as 90% of all businesses, whether governmental or private take place through the internet and computer media.

Affordability and Cost:

Implementing network security and backups can be daunting because of the price and confusing because of the technology. However, it is essential to invest both the time and money to understand and implement a secure system. While doing so may be costly, the alternative is living with the risk that the data or network could be compromised or destroyed at any time. The cost of a secure network needs to be weighed against the cost of a data breach or corruption, and its impact on the company. With the vast array of networking tools and services



available, it is also possible to develop a secure network on a budget. IT professionals are trained to keep cost in mind when recommending and building networks.

Advantages Available to Organisational Hackers:

All indicators point to cyber crime becoming a larger and more serious threat to companies. This is possible due to the following faults and negligence on the part of the management of the organisations:

Mis-configured Firewalls: Despite developments in the usability of firewall technology, many professionals still do not have the knowledge to maintain their own firewalls or verify the work of consultants.

Servers with No Specific Protection: Servers often share a single administrative password across a domain, and only have the most rudimentary anti-virus software installed. Anti-virus software does not protect servers from hacker-based attacks, and a single admin- password further multiplies risk.

Poorly Managed Operating System and Application Patching: In many companies it could be a full-time job, applying application and operating system patches. Every unique missed patch is vulnerability for hackers to exploit. Companies must employ strategies for installing and validating patches across all IT assets.

Shaky Account Administration: Dead accounts are often left active on systems; even if this is only for a couple of weeks, it could give a hacker or a disgruntled ex-administrator all the opportunity they need. IT professionals must educate and work closely with HR departments to ensure that processes are in place for effective account management.

Logs For The Sake Of Logs: Firewalls and security applications produce log files that are often large and difficult to read. For administrators it is often easier to find something else to do, rather than trawl through reams of paper. Companies can circumvent this by employing applications that take a proactive and preventative approach to security rather than just telling users something is wrong.

Some of the simplest things are still making life very easy for hackers. For many IT professionals there just isn't enough time in the day to effectively manage patching and account administration, so it is easy to see why things get forgotten and holes start to develop. The lack of server protection is of particular concern, given that this is a hacker's ultimate destination. Poorly administered firewalls and patching is like leaving the front door unlocked, but failing to adequately protect a server is tantamount to sitting a hacker down at it and asking if they'd like a hand. It is essential for organizations to take a structured, layered and proactive approach to network security.

3. *Types of Cyber Crimes:*

Hacking: In this category, a person's computer is broken into so that his personal or sensitive information can be accessed. This is different from ethical hacking, which many organizations



use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location. Many crackers also try to gain access to resources through the use of password cracking softwares. Hackers can also monitor what users do on their computer and can also import files on their computer. A hacker could install several programs on to their system without their knowledge. Such programs could also be used to steal personal information such as passwords and credit card information.

Theft:

This type of cyber crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the government authorities. Nowadays, the justice system is addressing this cybercrime and there are laws that avert people from unlawful downloading.

Cyber Stalking:

This is a type of online harassment wherein the victim is endangered to a barrage of online messages and emails. Normally, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk to make the victims' lives dejected.

Identity Theft:

This is a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card, full name and other sensitive information to drain off money or to buy things online in the victim's name. The identity thief can use person's information to fraudulently apply for credit, file taxes, or get medical services. It can result in major financial losses for the victim and even spoil the victim's credit history.

Malicious Software:

This software, also called computer virus, is Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to gather sensitive information or data or causing damage to software present in the system. Examples are spreading of virus or Trojan horse, and spreading of other malicious codes.

Child soliciting and Abuse:

This is also a type of cyber crime in which criminals solicit minors via chat rooms for the purpose of child pornography.

Computer vandalism:

It is a type of cybercrime that Damages or destroys data rather than stealing. It transmits virus.



Cyber terrorism:

It is a use of Internet-based attacks in terrorist activities. Technology savvy terrorists are using 512-bit encryption, which is impossible to decrypt.

Software piracy:

It is a theft of software through the illegal copying of genuine programs. Distribution of products intended to pass for the original. If an individual with a single user license loads the software onto a friend's machine, or if a company loads a software package onto each employee's machine without buying a site license, then both the single user and the company have broken the terms of the software license agreement and are therefore guilty of software piracy. Software piracy involves the unauthorized use, duplication, distribution, or sale of commercially available software. Software piracy is often labelled as soft lifting, counterfeiting, Internet piracy, hard-disk loading, OEM un-bundling, and unauthorized renting.

IPR Violations:-

These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations, etc.

Cyber Squatting: Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber Squatters register domain names identical to popular service provider's domain so as to attract their users and get benefit from it.

Denial of service attacks: This crime is committed by the criminal, who floods the bandwidth of the victim's network or fills his e-mail box with spam-mail depriving him of the services he is entitled to access.

Cyber Bullying:

Bullying has long been of concern to school officials and parents alike. Bullying, which is a type of aggressive behaviour, has now entered the electronic age in the form of cyber bullying (e.g., e-mails, text messages, profile sites). Efforts to combat cyber bullying include prevention and intervention programs at the community, school, and family levels. Majority of U.S. states have written legislation to address bullying and cyber bullying and many schools have established policies that prohibit electronic bullying and developed consequences for doing so.

E-commerce/ Investment Frauds:-

Sales and Investment Frauds: An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. This fraud is attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.



Sale of Illegal Articles:-

This would include trade of narcotics, weapons and wildlife, etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

Online Gambling:-

There are millions of websites hosted on servers abroad that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money-laundering.

Defamation:

Defamation can be understood as the intentional infringement of another person's right to his good name. *Cyber Defamation* occurs when defamation takes place with the help of computers and/or the Internet, e.g., someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. Information posted to a bulletin board can be accessed by anyone. Cyber defamation is also called as *cyber smearing*.

Data Diddling:

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data. It also includes automatic changing of the financial information for some time before processing and then restoring original information.

Theft of Internet Hours:

This includes unauthorized use of Internet hours paid for by another person. By gaining access to an organisation's telephone switchboard (PBX), individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties. Additional forms of service theft include capturing 'calling card' details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards.

Theft of Computer System (Hardware):

This type of offence involves the theft of a computer, some part(s) of a computer, or a peripheral attached to the computer.

Physically Damaging A Computer System:

This includes physically damaging a computer or its peripherals, either by shock, fire or excess electric supply, etc.

Breach of Privacy and Confidentiality:

Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc. Confidentiality means non disclosure of information to



unauthorized or unwanted persons. Leakage of personal information or some other type of information which is useful for business to other persons may cause damage to business or person. Such information should be carefully and zealously protected.

4. *Fighting Cyber Crime in Different Countries:*

Owing to the world-wide impact of cyber crime, various countries are using legal, organizational, and technological approaches to fight against it. *Legal approach* aims to restrict cyber crime activities through legislation. *Organizational approach* aims to enforce laws, to promote cooperation, and to educate the public through the establishment of dedicated organizations. *Technological approach* aims to increase the effectiveness of the technological components that comprise the cyberspace, by way of conducting continuous research in that direction, in order to better equip them to withstand the onslaught of the damaging effects of cyber crime.

5. *Legal Framework for Protection from Cyber Crime:*

International Legal Protection from Cyber Crime:

Cyber crime law includes laws related to computer crime, internet crime, information crimes, communications crimes and technology crimes. Cyber crime laws create the offences and penalties for cybercrimes. Cyber crime is a global problem, which requires a coordinated international response.

International cyber crime conventions:

- African Union Convention on Cyberspace Security and Personal Data Protection
- Council of Europe Convention on Cybercrime (also known as the Budapest Convention on Cyber crime)

Some Specific Cyber Crime Laws:

Cyber crimes Bill- South Africa (South Africa signed the Budapest Convention in 2001)

Cyber Security Information Sharing Act (CISA) - United States of America

Criminal Code Act, 1995- Australia

Cyber crime Act, 2001- Australia

Criminal Code of Canada

Cyber Security Law- China

Criminal Code of France

Computer Crimes Act- Malaysia

Crimes Act, 1961, New Zealand

Cyber crime Prevention Act of 2012 – Philippines

Act on Computer Crimes- Thailand

Cyber crimes Act, 2015- Tanzania

UK- Computer Misuse Act, 2013

United States Code-USA



President Barack Obama released an executive order in April, 2015, to combat cyber crime. The executive order allows the United States to freeze assets of convicted cyber-criminals and block their economic activity within the United States. This is one of the first solid legislation that combats cyber crime in this way.⁶

The European Union adopted directive 2013/40/EU. All offences of the directive, and other definitions and procedural institutions are also in the Council of Europe's Convention on Cyber crime.⁷

Legal Protection from Cyber Crime in India:

Information Technology Act (IT Act), 2000, and Information Technology (Amendment) Act (IT (Amendment) Act), 2008:

The above two pieces of legislation form the bedrock of cyber law infrastructure in India. The Information Technology (IT) Act, 2000, was passed by the Indian Parliament in May, 2000, and came into force in October of the same year. Its prime purpose is to provide the legal infrastructure for e-commerce in India. It was the first legal instrument to provide legal sanctity to electronic records and contracts expressed through electronic means of communication. The Act was later amended in December, 2008, through the IT (Amendment) Act, 2008.

Cyber crime is not a defined term but a catch-all phrase attributable to any offence involving an internet device. Most of the cyber crimes are listed under the Information Technology Act (IT Act), 2000, which was amended in 2008.

However, this clarity vaporises with the realisation that IT Act is not the only enactment covering cyber crime. The Indian Penal Code (IPC) could also be called in to initiate prosecution against cyber crimes or to supplement the provisions of the IT Act. For instance, offences like hacking, data theft, virus attacks, denial of service attacks, illegal tampering with source codes including ransom ware attacks could be prosecuted under S.66, r/w., S.43 of the IT Act. Cases of forging a credit or debit card or even cloning a mobile SIM with dishonest or fraudulent intent to cause wrongful loss or wrongful gain could be prosecuted under IPC provisions (S.463 to S.471 IPC, as applicable).

Additions to the IT Act in 2008 include protection against identity theft (S.66C) or cheating by impersonating online (S.66D). Victims of revenge porn may register complaints for violation of their privacy under S.66E, as also under S.67 and S.67A of the IT Act, in addition to IPC provisions. S.67A and S.67B also provide for prosecution of pornography and child pornography respectively. In case of the latter, the provisions of the Prevention of Children from Sexual Offences Act, 2012 (POCSO) may also be invoked.

As children are armed these days with cameras and data on their mobile phones at increasingly reducing prices, and raging hormones, the instances of revenge-porn attacks by children against children are on the rise. Irrespective of the age of the accused, if the offence of circulating sexually explicit content or violating privacy through dissemination of images or



videos of private parts, is committed, the person is susceptible to prosecution. With respect to child-pornography, the law is very stringent. It is not only publishing or transmission of child porn that is an offence but even browsing for such content and retaining or downloading it is an offence too, unlike for pornography where only the dissemination and transmission, sale, etc. are considered offences. Most offences carry maximum imprisonment of three years and fine. However, the more serious offences such as child pornography carry stronger punishment ranging from five to seven years. Crimes other than those affecting the “socio-economic conditions” or against women and children, may also be compounded, i.e., settled.

Offence Sections under the IT Act 2000:

- Tampering with Computer Source Documents (S.65)
- Hacking with Computer Systems (S.66)
- Publishing false Digital signature (S.73)
- Breach of Confidentiality & Privacy

Computer Related Crimes Covered Under IPC And Special Laws:

- Sending threat messages through e-mail (S.503)
- Forgery of Electronic records (S.463- IPC)
- E-mail spoofing (S.463- IPC)
- Web Jacking (S.383- IPC)
- Online sale of Drugs (Narcotics & Drugs prevention Acts)

Reporting a Cyber Crime:

The procedure for reporting cyber crimes is more or less the same as for reporting any other kinds of offences. The local police stations can be approached for filing complaints just as the cyber-crime cells specially designated with the jurisdiction to register complaint. Apart from this, provisions have now been made for filing of 'E-FIR' in most of the states. In addition, the Ministry of Home Affairs is also launching a website for registering crimes against women and children online including cyber crimes.

If a police station refuses to register the complaint, a representation may be given to the commissioner of police/superintendent of police. If in spite of that action is not taken, the next step could either be a private complaint before the concerned Court or a Writ before the High Court. In general, there is still a lot of inertia in registration and investigation of cyber crimes. This does affect collation of electronic evidence and containment of damages, whether the offence is against an individual or a business.

Remedies for Cyber Crime:

Apart from the criminal processes, Section 46 of the IT Act also provides for remedies against data theft, hacking, virus attacks and financial frauds covered under Chapter IX (S.43 to S.45) by filing an application before the adjudicating officer.



Businesses also have to take into account possibility of being held liable for data protection violations (S.43A & S.72A of the IT Act). Apart from the possibility of civil and criminal actions being initiated against them, if they fail to report cyber security incidents to the central authority, they would be liable for action. Being themselves victims of cyber crimes will not help them wriggle out of this requirement. Further, businesses which fall within the category of “intermediaries” have very heavy responsibilities and duties under the IT Act.

The ambiguities:

Several initiatives have been taken to ensure awareness among police and judiciary. These exercises have to be balanced with sensitisation programmes to ensure that the persons involved in the system understand the effects of cyber crime and act expeditiously. There are, however, many old systemic problems. Also, there is rampant abuse and misuse of the provisions of the IT Act due to its opacity. Lack of awareness among users highly aggravates this problem.

One instance is of WhatsApp administrators being threatened with criminal prosecution for posts made in groups. S.79 of the IT Act clearly exonerates persons who have no control over the content posted and the only liability is for complying with the intermediary rules. This would also apply to WhatsApp, the service provider, and not the person starting a group. Ambiguity is merely being misused in such instances.

Other instance where there is actually no ambiguity in law and yet it is being misused is of S.67 being used to prosecute “cyber defamation”. S.67 is on par with S.292 of IPC, and both have clearly defined high thresholds for initiation of action. This section was neither intended for nor does it apply to “cyber defamation”. Clearly, after ensuring strike-down of S.66A of the IT Act through its rampant abuse, the enforcement authorities have now resorted to S.67 of the IT Act. Such instances of patent abuse merely dilute the effectiveness of the provisions.

Infrastructure to Fight Cyber Crime in India:

India’s first exclusive cyber crime enforcement set-up was the Cyber Crime Police Station set up in Bangalore.

This was followed-up by a similar police station in Andhra Pradesh, which functions from Hyderabad city and has state-wide jurisdiction.

Cyber Crime Investigation Cells have also been set up by police departments of Mumbai, Kolkata and Tamil Nadu.

Law of which country is to be applied to a particular Cyber Crime: A Paradox:

A hacker sitting in Iceland may use a proxy in Thailand to hack into servers of the London Stock Exchange. It is a dilemma as to which country’s cyber laws apply in this instance. The decentralised nature of the crime makes it that much tougher to demarcate jurisdiction. This situation is further compounded by the fact that cyber laws are not consistent across nations (what may be a cyber crime in India may be perfectly legal in Sri Lanka). For instance,



the provisions of the Indian IT Act, 2000, apply not only to the whole of India, but also to offences committed outside Indian territory as well, provided the offence involves a computer, computer system, or a computer network located in India.

A serious drawback of current cyber crime legislation is that all offences, except cyber-terrorism, are bailable. This allows ample leeway for guilty individuals to destroy all electronic evidence of their crimes as soon as they have attained bail. This casual approach to cyber crime has led to most people, as well as enforcement agencies, to lose faith in the legislation, and contributed to the extremely low conviction rate. Hence, one cannot really blame the inspector at your neighbourhood for not being too keen on registering a cyber crime case. Thus, the situation is deplorable.

Women's victimization in cyberspace should be scrutinized separately since unfortunately, women are often more vulnerable than men, even in the developed countries. Cyber crime has a greater adverse effect on women than on men. Due to such offenses women feel humiliated. Libel and disclosure of confidential information can cause stigmatization and undermine the reputation of women.

Factors contributing to the increase of cyber crimes include the ability of offenders to use pseudonyms, women behaviour in cyberspace (for example, visiting sites with sexual content), failure to report about cyber crimes to the authorities, etc. Motives of cyber crimes against women include personal enmity, professional jealousy, sexual motives, self-affirmation, wish to defend particular point of view, as well as, to test skills and knowledge of Internet technologies.

International Legal Protection Efforts for Women:

Article 17 of *International Covenant on Civil and Political Rights* (1966) prohibits "arbitrary or unlawful interference with privacy, family, home or correspondence, or unlawful attacks on honour and reputation". *European Convention on Cyber Crime* also contains many important rules. However, it is necessary to adopt a comprehensive Act to protect the rights of women in cyberspace, since majority of cyber crimes are committed because of the absence of such legislation.

Legal Protection Efforts for Women in India:

Let us examine the criminal law protection of women's rights on the virtual space in India.

Section 66A of the IT Act (as amended on 23-12-2008) prohibits sending by means of a computer resource or a communication device, any information that is grossly offensive or has menacing character, or persistently sending any false information for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will. It is also punishable to send any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience, or to deceive or to mislead the addressee



or recipient about the origin of such messages. Section 66E outlaws capturing, publishing or transmission of the image of private area of any person without his or her consent. Section 67 provides punishment for publishing or transmitting obscene material in electronic form. Section 509 of Indian Criminal Code prohibits words, gestures or acts intended to insult the modesty of a woman.

Thus, the author emphasizes that freedom of speech is not guaranteed by the Constitution in the case of indecent behaviour. The author believes that the laws of various countries are not able to protect efficiently the rights of women in cyberspace. Thereby, the author suggests that international organizations, including the United Nations, as well as scientific organizations should continue to study the behaviour that infringes the rights of women in cyberspace, for improving existing legislation in order to protect women as the most vulnerable social group.

7. *Suggestions to Combat and Circumvent Cyber Crime:*

Ways to Prevent Cyber Crimes against Individuals:

Computer users must use a firewall to protect their computer from hackers. Most security software comes with a firewall. They must turn on the firewall that comes with their router as well. Computer users are recommended to purchase and install anti-virus software such as Norton Anti-Virus, etc. It is advised by cyber experts that users must shop only at secure websites. They should look for a Truste or VeriSign seal when checking out. They should never give their credit card information to a website that looks suspicious or to strangers.

Users must develop strong passwords on their accounts that are difficult to guess. One way is to include both letters and numerals in their passwords. They must continuously update passwords and login details. By changing login details, at least once or twice a month, there are less chances of becoming a target of cyber crime. It is suggested to monitor children and how they use the Internet. Parental control software must be installed to limit where they can surf.

Users must make sure that social networking profiles such as Facebook, Twitter, YouTube, MSN are set to private. They must regularly check their security settings and be careful what information they post online. Once it is on the Internet, it is extremely difficult to remove. Users must secure their mobile devices. More often than not, people leave their mobile devices unattended. By activating the built-in security features, they can avoid any access to personal details. They must never store passwords, pin numbers and even own address on any mobile device. Users must protect their data to prevent criminals from hacking. They must use encryption for most sensitive files, such as tax-returns or financial records, make regular back-ups of all important data, and store them in a different location. Users must be alert while using public Wi-Fi Hotspots. While these access points are convenient, they are far from secure. They must avoid conducting financial or corporate transactions on these networks.



Users must protect their e-identity. Users must be careful when giving out personal information such as name, address, phone number or financial information on the Internet. They must make sure that websites are secure.

Users must avoid being scammed: It is suggested that users must assess and think before they click on a link or file of unknown origin. They must not open any emails in inbox. They must check the source of the message. If there is a doubt, they must verify the source. They must never reply to emails that ask them to verify information or confirm their user ID or password.

Ways to Overcome Organisational Cyber Crime:

Organisations must be encouraged to partner with, law enforcement officials who can put the cyber-criminals behind bars, and government officials who create the laws and regulations required to arrest them.

Organizations need to establish enterprise-wide risk management programmes, overseen by either their chief executive officer or a chief risk officer reporting to the CEO. Too many companies are making a mistake by managing risks in different departments.

Organizations must address the cyber issue comprehensively if they are to survive and not impede their growth. ***According to Barr, every company also should:***

Establish a risk management council, which would bring together representatives from finance, legal, human resource, communications, line operations and other departments.

Create a culture, policies and procedures that encourage or direct every employee to play a role in identifying and managing risk.

Analyse their inter-dependencies. In other words, consider what would happen if an unprepared supplier or business partner or even customer were to experience a business interruption or go out of business due to a cyber or other disaster. Additionally, determine what measures these companies have taken to protect themselves.

Develop contingency-management and disaster recovery plans that address cyber crime incidents, natural catastrophes and other disasters.

90% of security issues can be addressed by focusing on the basics and most of what one needs, one already has available. Basic controls should have been in operation, for example, the need to install the latest versions or patches for operating systems, which would close many of the gaps that are exploited by hackers. Amongst all the defences such as keeping firewalls in restrictive mode and keeping operating systems patched to the latest version, there are many straightforward ones that should already be in force such as a properly promulgated information security policy, documented disaster recovery plans, the changing of all default passwords, reviewing of logs, and persistence of reviews and auditing.



Businesses ought to increase awareness of the potential of technologies and the threats they pose. They should not only protect themselves against these threats but must also have clear processes for ensuring quick bounce-back after an attack. Hygiene in the digital world is as important as in the real and may protect both individuals and businesses alike in alleviating the harm that a cyber attack may cause.

Improvement in Legal Provisions to Prevent Cyber Crime:

Legal provisions should be framed in such a way as to provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals.

- . Expeditious action by police in clear cases of cyber crime; collation of evidence in a manner that will withstand trial, and completion of Court proceedings without delay with clear understanding of the technology and the law, are just some goals that the system could aim for. Law cannot ask users to “keep away” from use of technologies merely due to its inability to protect them. That is akin to asking women to not step out after dark. Until the legal system demonstrates robustness, even irrespective of it, users must exercise due caution in the use of technology. Adapt, but do so with care and responsibility, as the virtual world requires as much caution as the real world.

8. *Conclusion:*

In brief, cyber crime is evolving as a serious threat. A cyber-attack is an attack originated from a computer, against a website, computer system or individual computer that compromises the confidentiality, integrity or availability of the computer or information stored on it. Due to the fact that existing laws in many countries are not tailored to deal with cyber crime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. World-wide, governments, police departments and intelligence units have begun to react against cyber crime. Many efforts are being taken at international level to curb cross-border cyber threats. Indian police have started special cyber cells across the country and have started educating the peoples so that they gain knowledge and protect themselves from such crime.

Computer technologies have eroded the nation-state's ability to enforce criminal laws, as they apply to attacks on communications between computers, on data stored on computers and on real-world systems that are controlled by computers. These attacks elude the efforts of national law enforcement agencies and pose a serious threat to national economies and infrastructures.⁸ The enforcement problem presented by these attacks demonstrates that society needs to rethink how it should enforce criminal laws to prevent computer-mediated crime. Our current model of criminal law enforcement, with its origins in real-world urbanisation, does not, and cannot, meet the needs of protecting society from cyber crime.

The society's current law enforcement model is inadequate. The nation-states can control cyber crime more effectively by replacing the current, hierarchical model with a system



of “distributed” security that uses criminal sanctions to require (i) computer users, and (ii) those who provide access to cyber-space, to employ reasonable security measures to prevent the commission of cyber crimes. Criminal sanctions are preferable to civil liability, in this context.

References:

1. Moore, R. (2005) *“Cyber crime: Investigating High-Technology Computer Crime,”* Cleveland, Mississippi: Anderson Publishing.
2. Warren G. Kruse, Jay G. Heiser (2002). *“Computer forensics: incident response essentials.”* Addison-Wesley. p. 392. ISBN 0-201-70719-5.
3. Halder, D., & Jaishankar, K. (2011) *“Cyber crime and the Victimisation of Women: Laws, Rights, and Regulations.”* Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.
4. Steve Morgan (January 17, 2016). *“Cyber Crime Costs Projected To Reach \$2 Trillion by 2019”.* Forbes.
5. Cybercrime – what are the costs to victims – North Denver News.
6. Northam, Jackie. *“U.S. Creates First Sanctions Program Against Cybercriminals”.*
7. Adrian Cristian MOISE (2015). *“Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level”* (PDF). *Journal of Law and Administrative Sciences*.
8. See, e.g., Spencer Swartz, *Secret Service: Internet Fraud Threatens U.S. Economy*, http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-02-18-fraud-threat_x.htm (Feb. 18, 2005).



PRIVACY AND SECURITY ISSUES IN CLOUD COMPUTING

Mr. Rohit Mishra

Associate, Cognizant Technology Solutions

1. Introduction

The National Institute of Standards and Technology (NIST) Special Publication 800-145 (NIST SP 800-145) defines the cloud as the hardware and software infrastructure required to provide “on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.” These characteristics allow for three service models: software, platform, and infrastructure (Mell and Grance, 2011). Most will agree that any computing model that qualifies as cloud computing must at minimum have the following criteria:

Elasticity

Cloud computing is typified by its ability to rapidly scale the capacity of the provided service up or down with little to no interaction from the consumer. This characteristic, known as *elasticity*, is key to cloud computing. In some delivery models of cloud computing, elasticity is often facilitated through virtualization, although cloud computing does not require virtualization.

Multitenancy

Even private clouds, which run the workload of a single corporation possess multiple tenants, be they workloads or individual users. This multitenancy and multitenant amortization of the shared compute resource is part of the reason for the economic benefits of cloud computing.

Economics

With cloud computing services, the expectation is that the consumer is charged for the amount of time used on the resource. Cloud computing changes the computing barrier to entry for high performance computing resources, by allowing consumers to use only what they need for the time in which they need it. In turn, this has allowed organizations to effectively respond to peak demand requirements without having excess compute resources sitting idle during dormant periods. Clouds can achieve this by distributing the load across multiple shared resources and relying on economies of scale.

1.1 Cloud Computing service layers

Cloud computing providers provide different kinds of services to cloud computing consumers. In order to understand the different layers of service, it's important to understand how they would relate in a no cloud computing scenario. The image below compares cloud and no cloud based systems.

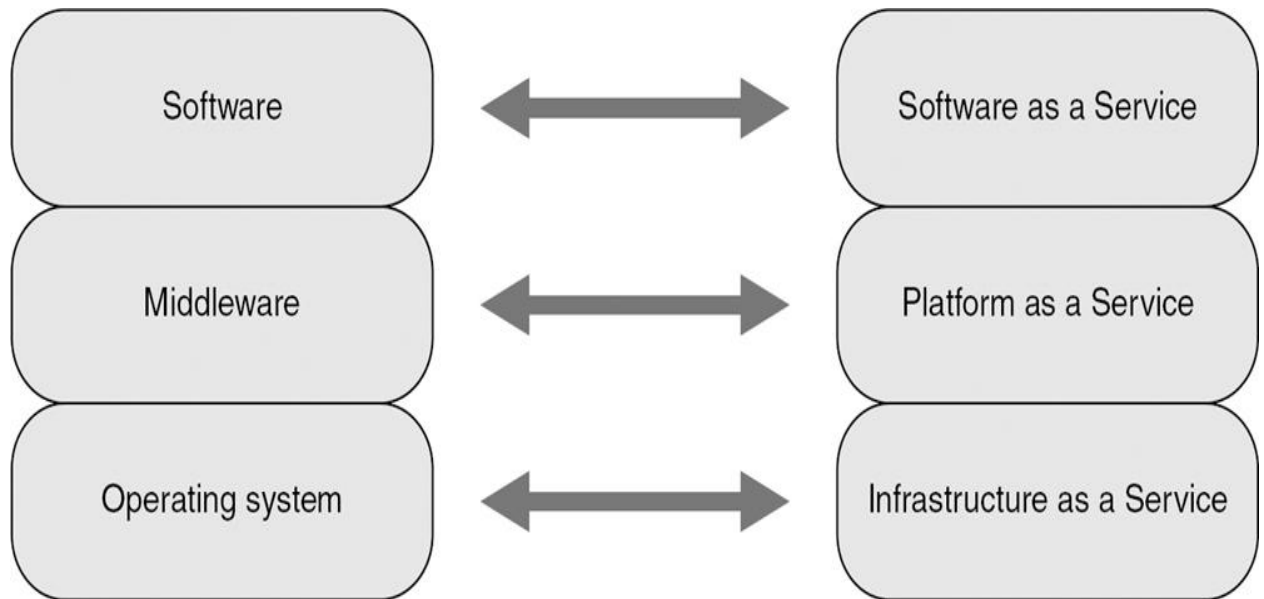


Figure 1: Traditional Model versus Cloud Computing Model

1.1.1 Infrastructure as a Service

Infrastructure as a Service (IaaS) providers allow their customers access to different kinds of infrastructure. The provider typically provides this service by dividing a very large physical infrastructure resource into smaller virtual resources for access by the consumer. One of the more popular IaaS providers is Amazon, who provides their EC2 IaaS.

1.1.2 Platform as a Service

Platform as a Service (PaaS) providers extend the software stack provided by IaaS to include *middleware*. Middleware generically refers to software such as a DB2 database, or runtime environments such as a Java Runtime Environment (JRE) or a WebSphere application server. This middleware is a prerequisite to running more sophisticated applications, and provides a rich operating environment for the application to exploit. A popular example of a PaaS is Microsoft's Windows Azure platform.

1.1.3 Software as a Service

Application as a Service, or Software as a Service (SaaS) providers as they are more commonly known, typically provide a rich web-based interface to their customers. The customer, in most cases, is completely abstracted from the nuances of the application running behind the scenes. Tenant separation is often done at the application layer, leaving a common application, platform, and infrastructure layer underneath. Popular examples of SaaS include Google Apps.

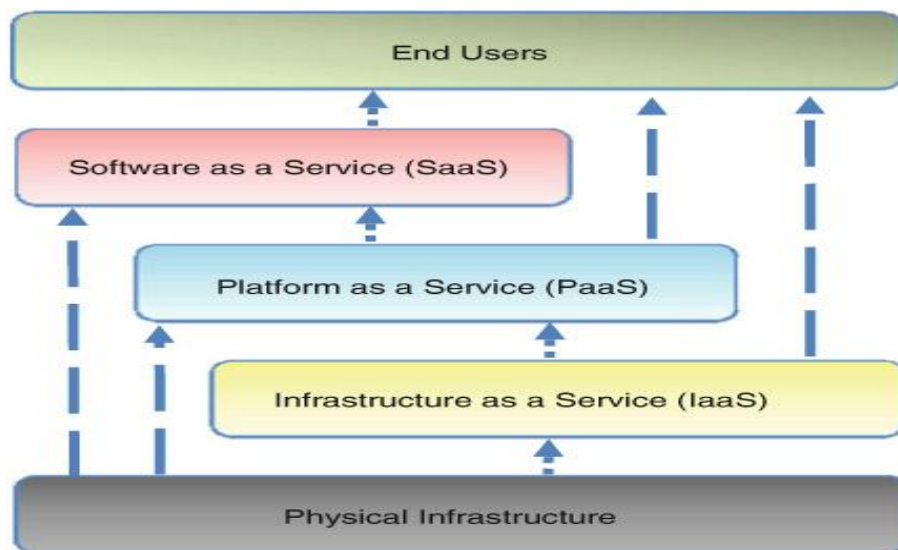


Figure 2 Cloud Computing Service Layers

2. Privacy Issues for Cloud Computing

Current cloud services pose an inherent challenge to data privacy because they typically result in data being exposed in an unencrypted form on a machine owned and operated by a different organization from the data owner. The major privacy issues relate to trust (e.g. whether there is unauthorized secondary usage of PII), uncertainty (ensuring that data has been properly destroyed, who controls retention of data, how to know that privacy breaches have occurred and how to determine fault in such cases) and compliance (in environments with data proliferation and global, dynamic flows and addressing the difficulty in complying with trans-border data flow requirements). When considering privacy risks in the cloud, as considered already within the introduction, context is very important as privacy threats differ according to the type of cloud scenario. For example, there are special laws concerning treatment of sensitive data, and data leakage and loss of privacy are of particular concern to users when sensitive data is processed in the cloud. Currently, this is so much of an issue that the public cloud model would not normally be adopted for this type of information. More generally, public cloud is the most dominant architecture when cost reduction is concerned, but relying on a CSP to manage and hold one's data in such an environment raises a great many privacy concerns. Privacy concerns in cloud computing can be related to below reasons:

2.1 Lack of User Control

User-centric control seems incompatible with the cloud: as soon as a SaaS environment is used, the service provider becomes responsible for storage of data, in a way in which visibility and control is limited. So how can a consumer retain control over their data when it is stored and processed in the cloud? This can be a legal requirement and also something users/consumers want—it may even be necessary in some cases to provide adequate trust for consumers to switch to cloud services.



2.2 Lack of Training and Expertise

Deploying and running cloud services may necessitate many jobs requiring high skills, but lack of STEM (science, technology, engineering, and mathematics) graduates in Europe and other parts of the world could make it difficult to recruit suitably qualified people. In particular, lack of trained personnel can be an issue from a security point of view.

2.3 Unauthorized Secondary Usage

There is a risk (and perhaps even an expectation!) that data stored or processed in the cloud may be put to unauthorized uses. It is part of the standard business model of cloud computing that the service provider may gain revenue from authorized secondary uses of users' data, most commonly the targeting of advertisements. However, some secondary data uses would be very unwelcome to the data owner (such as, e.g. the resale of detailed sales data to their competitors). Therefore, it may be necessary for consumers and CSPs to make legally binding agreements as to how data provided to CSPs may be used. At present, there are no technological barriers to such secondary uses, although as we consider further in various chapters in this book, it is likely that in future such agreements might be enforceable in a technological sense. This will help enhance trust and mitigate the effects of the blurring of security boundaries.

2.4 Complexity of Regulatory Compliance

Due to the global nature of cloud computing and the many legislations in place around the world, it can be complex and difficult to ensure compliance with all the legislation that may apply in a given case.

Location matters from a legal point of view as different laws may apply depending on where information exists, but in cloud computing, the information might sometimes be in multiple places simultaneously; it may be difficult to know exactly where it is or it may be in transit. A complicating factor is that there are multiple copies of data located in the cloud. Furthermore, these copies can be managed by different entities: a backup SP, a provider used to respond to peak capacity needs, specialized services, etc.

3. Security Issues in Cloud Computing

Security often tops the list of cloud user concerns. Cloud computing presents different risks to organizations than traditional IT solutions. There are a number of security issues for cloud computing, some of which are new, some of which are exacerbated by cloud models and others that are the same as in traditional service provision models. The security risks depend greatly upon the cloud service and deployment model. For example, private clouds can to a certain extent guarantee security levels, but the economic costs associated with this approach are relatively high.

At the network, host and application levels, security challenges associated with cloud computing are generally exacerbated by cloud computing but not specifically caused by it. The main issues relate to defining which parties are responsible for which aspects of security. This division of responsibility is hampered by the fact that cloud APIs are not yet standardized. Customer data security raises a number of concerns, including the risk of loss, unauthorized collection and usage and generally the CSP not adequately protecting data.



4. Tools for Privacy and Security

Cloud data storage and services will continue to grow. More people and companies will keep more of their confidential data in the cloud. With more people having more confidential data in the cloud will come a greater awareness of the vulnerability of personal data. This greater awareness of cloud data privacy and security will manifest itself in the following areas:

4.1 Encryption by Default

Google and Apple now encrypt the data that they store on devices by default. Expect default encryption to become standard for cloud storage providers. Note that this encryption applies to data on the device itself and not to data backed up to cloud storage. These providers still have the ability to give the unencrypted data in response to law enforcement requests (Kravets, 2014). This also means your cloud data remains vulnerable to attackers and malicious insiders with access to the data center servers.

4.2 Two-Factor Authentication

Two-factor authentication might not have the success that was anticipated because many perceive it as an inconvenience that requires a second step and the dependency on an additional hardware device. The device associated with the two-factor authentication could get broken, lost, stolen, or left somewhere; all of which mean not having access to cloud data. While backup codes, multiple trusted devices, and applications like Google Authenticator (<https://itunes.apple.com/app/google-authenticator>) or Authy (<https://www.authy.com/>) make it possible to remedy these situations, the hardware device requirement and management leaves many looking for easier ways to achieve data security.

4.3 Zero-Knowledge Encryption

Zero-knowledge encryption will compete with default encryption for securing cloud data. Recent incidents in the news about governments, companies, and criminals continue to erode the trust people have in cloud storage providers to manage data encryption. Cloud data storage providers will promote zero-knowledge encryption as the only real way to secure personal or corporate data. Companies especially will look to zero-knowledge encryption to protect their data (Vijayan, 2013).

4.4 Anonymity Networks

For those seeking to protect their cloud meta-data, anonymity networks like Freenet (<https://freenetproject.org/>), I2P (<https://geti2p.net/>), and Tor (<https://www.torproject.org/>) will grow in popularity. These anonymity networks allow for anonymous access to cloud storage. You must still encrypt the stored data, but the anonymity network prevents your provider from tracking your IP address or physical location. Tails (<https://tails.boum.org/>) provides a live operating system with Tor and other tools for anonymous Internet activity. Tails can be installed on and executed from a USB memory stick, leaving no trace on the host computer once Tails is shut down and the memory stick is removed. The creators of Tails have the goal of making anonymity online easily accessible to everyone anywhere.

4.5 Monetizing Security and Privacy



We expect to see growth in niche services that provide cloud data privacy. Data security comes at a price and free cloud data storage costs somebody. Cloud storage providers typically use free accounts to build a customer base to attract investors, show advertisements, and sell additional services. These activities, to do well, require user data, hence the need to collect information from user metadata and content. Reputable companies do not use this data maliciously. However, its existence makes it attractive to criminals and authoritarian governments.

Cloud storage providers could seek to increase sales with fee for accounts offering encryption and security compliance, e.g., Safe Harbor or HIPAA. Providers might offer free accounts with large amounts of unencrypted storage, and then encourage users to secure it with encryption for a fee. The assurance of compliance with independent security standards will also draw more businesses into using cloud data storage and services.

4.6 Home Clouds

Network Attached Storage (NAS) devices allow individuals and small businesses specially to have their own private cloud data storage. Security concerns will motivate many to provide their own cloud data storage solutions, both private and commercial. Physical control of both endpoints, devices and storage, does satisfy some security concerns, related to legal issues and insider access. However, it does place the burden of security on the owner of home/private cloud. In addition, it does not address data backup and storage location redundancy.

5. Conclusion

Responsible management of personal data is a central part of creating the trust to underpin adoption of cloud-based services and thereby to encourage customers to use cloud-based services. Cloud providers need to safeguard the privacy and security of personal and confidential data that they hold on behalf of organizations and users. In particular, it is essential for the adoption of public cloud systems that consumers and citizens are reassured that privacy and security is not compromised. It will be necessary to address the problems of privacy and security raised in this chapter in order to provide and support trustworthy and innovative cloud computing services that are useful for a range of different situations.

REFERENCES

- Aazam, M., Hung, P., Huh, N., 2014. Cloud of Things: Integrating Internet of Things with Cloud Computing and the Issues Involved. Proceedings of International Bhurban Conference on Applied Sciences & Technology. Islamabad, Pakistan, January 14-18, 2014.
- ACM, 2013. Quantum Memory 'World Record'
- BBC News, 2014. GCHQ's Robert Hannigan says tech firms 'in denial' on extremism.
- Cheng, C., Zhang, C., Qiu, X., Yang Ji, Y., 2014. The Social Web of Things (SWoT) Structuring an Integrated Social Network for Human, Things and Services. J. Comput. 9 (2)
- Vijayan, J., 2013. Cloud computing 2014: Moving to a zero-trust security model.



CRIME AGAINST WOMEN IN CYBER SPACE- AN ANALYSIS

Ms. G. Selvi,

*Assistant Professor, School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Perungudi,
Chennai, Tamil Nadu*

INTRODUCTION

The traditional Indian society places women in a very high regards, the Vedas glorified women as the mother, the creator, and one who gives life and worshipped her as a Devi or Goddess. However, in modern times women are viewed as sex objects, she is treated inferior to men in various societal spheres and functions; this has created a huge gender bias between the men and women.

Safety of women has always been an issue, especially in a country like India where crime rate against women is increase. In olden days, it was limited to roads or at place away from home. Home was the safest place for a woman to protect herself from being victimized, but nowadays home is also become a dangerous place, prone to crime against women. The convergence of computer networks and technologies has given birth to a common space called 'cyberspace'. Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. With the advancement in technology there is a steep increase in cyber crime and victimization of women and it poses a major threat to a person as a whole globally. India is among the very few countries to enact IT Act 2000 to curb cyber crimes. The study discusses in detail the various cyber crimes against women and the legal framework regulating these crimes in India. Finally the study provides with appropriate suggestions where necessary.

Cyber Crime

Cyber crime is a new type of crime that occurs in this Science and Technology years. There are a lot of definitions for cyber crime. According to Wikipidia.com cyber crime also known as computer crime that refers to any crime that involves a computer and a network. Cyber crime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. Besides that cyber crime can be defined as crimes committed on the internet using the computer as either a tool or a targeted victim¹ (Joseph A E, 2006). Computer can be considers as a tool in cyber crime when the individual is the main target of cyber crime. But computer can be considers as target when the crime is directed to the computer. In addition, cyber crime also includes traditional crimes that been conducted with the access of Internet. For example hate crimes, telemarketing Internet fraud, identity theft, and credit card

¹ <http://www.crime-research.org/articles/joseph06/>



account thefts. In simple word, cybercrime can be defined as any violence action that been conducted by using computer or other devices with the access of internet. This action can give harmful effects to other.

As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cyber crimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cyber crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. However, before you can understand more about this system, let us find out more about cyber crimes.

The term ‘**Cyber**’ became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Due to increase in the number of citizens, misuse of technology in the cyberspace was clutching up which gave birth to cyber crimes at the domestic and international level as well.

There is no statutory definition of cyber crime under Indian laws, including under the IT act. Cyber crime can be defined as-“Any illegal act fostered or facilitated by a computer, whether the computer is n object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime”¹A generalized definition of cyber crime may be “Unlawful acts wherein the computer is either a tool or target or both”²

The Information Technology Bill (1999) has defined the cybercrimes as: Whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document used for a computer, computer programme, computer system, or computer network, when computer source code is required to be kept or maintained bylaw for the time being in force [shall be punishable with a fine which may extend up to rupees two lakhs or with imprisonment up to three years, or with both].

With the blessings of Information and Communication Technology, the digital age is benefiting billions across the world. The entire world has become a global village. Internet has proved to be the greatest invention to mankind. However, the transcendental jurisdiction of Internet has

¹ definition by royal Canadian mounted police in 2000, as quoted in amer hinduja- computer crime investigations in the united states- leveraging knowledge from the past to address the future, international journal of cyber criminology, vol. 1, issue 1, January,2007

² Roshan, N., What is cyber Crime. Asian School of Cyber Law, 2008: Access at http://www.http://www.asclonline.com/index.php?title=Rohas_Nagpal



caused the major threat to the society in the form of cybercrimes. Women and children are the main victims of this transgression.

Categories of Cyber Crime

Cyber crimes are broadly categorized into three categories, namely crime against

1. Individual
2. Property
3. Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

Individual: This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and “grooming”. Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

Property: Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person’s bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization’s website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

Types of cyber crime that are committed against women:

Amongst the various cyber crimes committed against individuals and society at large the crimes which can be mentioned as specially targeting women are as follows: –

1. Harassment via e-mails.
2. Cyber-stalking.
3. Cyber pornography.
4. Defamation.
5. Morphing.
6. Email spoofing.

Most cyber crimes are of general nature and they target men and women alike. But there are certain cyber crimes that are more likely to target women than their male counterparts. These include cyber stalking, cyber harassment, morphing and obscene publication, email/profile hacking, spoofing, cyber pornography including revenge porn, internet voyeurism, cyber



defamation, cyber bullying, e-mail harassment, cyber blackmailing, threatening, emotional cheating by impersonation, intimate partner violence through internet and abetment of such offences.

Cyber harassment- “ a course of conduct directed at a specific person that causes substantial emotional distress in such person amid serves no legitimate purposes” or “words, gestures, and actions which tend to annoy, alarm and abuse(verbally) other person.”

There are generally two types of harassment on the net-through electronic mail and during chats. These messages take many forms- inappropriate sexually explicit language, unwelcome questions about one’s physical appearance or sexual practices or threatening or hostile messages.

Morphing means editing the original picture by an unauthorized user or otherwise changing smoothly from one image/video to another by small gradual steps using computer animation techniques. As various morphing tools are widely available in internet, offenders often download girls' pictures from various social websites through real or fake profiles and then morph them. The morphed images may be used to blackmail the girl or her family by threatening to publish the morphed images. This amount to violation of IT act, 2000 and attracts Sections 43¹& 66¹ of the same. The violator can also be punished under IPC also for criminal

¹ Section 43 of the Information Technology Act, 2000: Penalty and compensation for damage to computer, computer system, etc. [If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, or computer resource –

1. accesses or secures access to such computer, computer system or computer network;
2. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
5. disrupts or causes disruption of any computer, computer system or computer network;
6. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;
7. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
8. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; steal, conceals, destroys or alters or causes any



trespass under section 441, section 290 for committing public nuisance, section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under section 501 for defamation.

Cyber stalking involves following a girl's movements across the internet by posting messages on the bulletin boards, discussion groups and entering the chat-rooms frequented by the girl, constantly bombarding the girl with emails, often threatening and abusive. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites and email². A cyber stalker relies upon the anonymity afforded by the internet to allow them to stalk their victims without being detected. The harassment can take on many forms, but the common denominator is that it is unwanted and often obsessive. Cyber stalking is often perpetrated not by strangers, but by someone a girl knows. It could be an ex, a former friend, or just someone who wants to bother a girl or her family in an inappropriate way. Cyber stalking can be terribly frightening. It alarms, torments, and terrorizes a girl. It can destroy friendships, careers, self-image, and confidence. If coupled with real-space stalking, cyber stalking can lead the victim into far greater physical danger including suicide attempts.

Cyber pornography The word Pornography literally means "Documenting a Prostitute" or "Depictions of acts of Prostitutes". It refers to portrayal of sexual material on the web. Criminals often rape or molest a girl, capture the incident by webcam or mobile phone and spread the video over internet. These incidents are becoming alarmingly common even in the rural areas of Bangladesh. Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens.

Section 67 of the IT Act is the most serious Indian law penalizing cyber pornography. Other Indian laws that deal with pornography include the Indecent Representation of Women (Prohibition) Act and the Indian Penal Code.

Further child pornography, which is aggravated form of pornography, is a much serious offence. The present Information Technology law enables the law enforcement agencies to take strict action against that seeking child pornography and its violation can lead to seven year term in jail and up to ten lakhs rupees fine³.

person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]

¹ Section 66 Computer related offences. -If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

² Smith, S.G., Chen, J., Basile, K.C., Gilbert, L.K., Merrick, M.T., Patel, N., et al. (2017). The National Intimate Partner and Sexual Violence Survey: 2010-2012 State Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention

³ Charandeep Singh Samrao, *Cyber Crimes* (Random Publications, Delhi, 2013)



Cyber defamation is publishing of defamatory material against another person with the help of computers or internet. If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation. The harm caused to a person by publishing a defamatory statement about him on a website is widespread and irreparable as the information is available to the entire world. Cyber defamation affects the welfare of the community as a whole and not merely of the individual victim. It also has its impact on the economy of a country depending upon the information published and the victim against whom the information has been published.

Email spoofing.

Email spoofing is a fraudulent email activity hiding email origins. The act of e-mail spoofing occurs when imposters are able to deliver emails by altering emails' sender information. Although this is usually done by spammers and through phishing emails for advertising purposes, email spoofing can have malicious motives such as virus spreading or attempts to gain personal banking information. The more common method used by men is to email vulgar photographs of themselves to women, praising their beauty, and asking them for a date or inquiring how much they charge for 'services'. Besides sending explicit messages via e-mail, SMS and chat, many also morph photographs - placing the victim's face on another, usually nude, body.

We have several laws to deal with cyber crimes and among them two enactments are important for practical purposes: the Information and Communication Technology Act, 2006 (ICTA) and the Pornography Control Act, 2012 (PCA). Cyber pornography can be prosecuted by section 8 of the PCA and also by section 57 of the ICTA. It will be extremely difficult to prosecute an act of morphing if the morphed image/video does not fall within the meaning of pornography. Acts of cyber stalking will probably continue to be immune from legal process as these laws do not specifically define them and our trial judges will rationally be reluctant to convict a person for acts not defined as crimes.

CAUSE FOR CYBER CRIME

1. Capacity to store data in comparatively small space:-

The computer has a unique characteristic of storing data in a very small space. This allows for much easier access or removal of information through either physical or virtual media.

2. Easy to access:-

The problems encountered in guarding a computer system from unauthorised access are that there is every possibility of unauthorised access not due to human error but due to the complex technology. By secretly implanted a logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilised to get past many security systems.



3. Complex-

The computers work on operating systems and these operating systems in turn are composed of millions of lines of code. The human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system using often more sophisticated means than originally anticipated by the systems engineers.

4. Negligence:-

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system. This negligence is usually a property of under resourced IT security provisions and the improvement of security barriers within software packages and network structures could lead to improved security.

5. Loss of evidence:-

Loss of evidence is a very common & obvious problem as all the data is routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

CYBER LAWS IN INDIA

Cyber crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cyber crimes.

The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

1. Cyber crimes under the IT Act :

- Tampering with Computer source documents - Sec.65
- Hacking with Computer systems, Data alteration - Sec.66
- Publishing obscene information - Sec.67,67A,67B,67C
- Un-authorised access to protected system Sec.70 Breach of Confidentiality and Privacy - Sec.72
- Publishing false digital signature certificates - Sec.73

2. Cyber Crimes under IPC and Special Laws:

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC



- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

3. Cyber Crimes under the Special Acts:

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
- Online sale of Arms Arms Act

IMPACT OF INFORMATION AND TECHNOLOGY ACT

The Information Technology Act, 2000 was passed by the Parliament on May 15, 2000, approved by the President on June 9, 2000 and notified to come into force on October 17, 2000. The Act, seeks to protect this advancement in technology by defining crimes, prescribing punishments, laying down procedures for investigation and forming regulatory authorities¹.

The Information Technology Act, 2000 initially consisted of XIII Chapters & 4 Schedules and 94 Sections. Two schedules have been deleted by the Information Technology (Amendment) Act, 2008. At present it has 2 Schedules. Chapters IX & XI covers up offences and penalties. The Information Technology Act, 2000 nor defines 'cyber crimes' neither uses this expression, but only provides the definition of and punishment for certain offences. Thus two kinds of definition of cyber crimes can be given. In narrow terms cyber crime consists of only those offences which are mentioned under the Information Technology Act, 2000, whereas broadly speaking cyber crime can be said to be an act of omission, commission or committed on or through or with the help of internet, whether committed directly or indirectly and which is prohibited by any law for which punishment corporal or monetary is provided. In this context it can be concluded that Information Technology Act, 2000 provides punishment for only certain offences and is not exhaustive of all cyber crimes.

The Information Technology (Amendment) Act, 2008 also added section 66A which prohibited the sending of offensive messages through a communication device (i.e. through an online medium). The types of information covered were offensive messages of a menacing character, or a message that the sender knows to be false but is sent for the purpose of 'causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will'. However, the provision was challenged on the ground of vagueness, arbitrariness and misuse and was ultimately struck down by the Supreme Court in the case of *Shreya Singhal*². In light of the sexual harassment, abuse and intimidation faced by women on the internet, the section could have provided for a proper remedy.

¹ K.P. Malik, *Computer and Information Technology Law* (Allahabad Law Agency, 2010.)

² *Shreya Singhal v. Union of India*, (2013) 12 SCC 73



As regards cyber victimization of women, the Information Technology law has remained a half baked law. Unfortunately even though Chapter XI of the IT Act deals with the offences such as Tampering with computer source documents (s.65), Hacking with computer system (s.66), publishing of information which is obscene in electronic form (s.67) Access to protected system (s.70), Breach of confidentiality and privacy (s. 72), Publication for fraudulent purpose (s.74) IT Act 2000 still needs to be modified. It does not mention any crime specifically as against women and children.

The basic problems, which are confronted with Cyber-Crimes, are Jurisdictional issues, Loss of evidence, Lack of Cyber Cops, Army and Cyber savvy judges who are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. The IT Act 2000 does not mention the typical cyber crimes like cyber stalking, morphing and email spoofing as offences. The Indian law is still unequipped to deal with various cyber offences against women such as revenge porn¹.

AFFIRMATIVE ACTIONS OF JUDICIARY

Ritu Kohli Case²

Ritu Kohli Case was India's first case of cyber stalking, in this case Mrs. Ritu Kohli complained to police against a person, who was using her identity to chat over the Internet at the website <http://www.micro.com/>, mostly in Delhi channel for four consecutive days. Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was also deliberately giving her phone number to other chatters encouraging them to call Ritu Kohli at odd hours. Consequently, Mrs. Kohli received almost 40 calls in three days mostly on odd hours. The said call created a havoc in personal life of the complainant consequently IP addresses was traced and police investigated the entire matter and ultimately arrested the offender. A case was registered under the section 509, of IPC and thereafter he was released on bail. This is first time when a case of cyber stalking was reported. Similar to the case of email harassment, Cyber stalking is not covered by the existing cyber laws in India. It is covered only under the ambit of Section 72 of the IT Act that perpetrator can be booked remotely for breach of confidentiality and privacy. The accused may also be booked under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again for outraging the modesty of women

¹ Debarati Halder and K. Jaishankar, *Cyber crimes against women in India*(TMC Academy Journal, Singapore. Vol 3, Issue 1, June 2008. pp. 48-62, 2008)

² <http://cyberlaws.net/cyberindia/2CYBER27.htm>



State of Tamil Nadu Vs Suhas Katti¹

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits. The court relied upon the expert witnesses and other evidence produced before it, including witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved and convicted the accused. This is considered as the first case in Tamil Nadu, in which the offender was convicted under section 67 of Information Technology Act 2000 in India.

The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the bank's computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

Avnish Bajaj vs. State²

This is famously known as Avnish Bajaj (CEO of bazzee.com – now a part of the e Bay group of companies) case.

Facts: There were three accused first is the Delhi school boy and IIT Kharagpur Ravi Raj and the service provider Avnish Bajaj.

The law on the subject is very clear. The sections slapped on the three accused were Section 292 (sale, distribution, public exhibition, etc., of an obscene object) and Section 294 (obscene acts, songs, etc., in a public place) of the Indian Penal Code (IPC), and Section 67 (publishing information which is obscene in electronic form) of the Information Technology Act, 2000. In addition, the School boy faced a charge under Section 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode.

¹ http://www.naavi.org/cl_editorial_04/suhas_katti_case.htm

² www.e-Mudhra.com



These offences invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first time conviction, and/or fines.

Held: In this case the Service provider Avnish Bajaj was later acquitted and the Delhi school boy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days

CONCLUSION

From the above discussion it seems quite clear that with the advancement of Information and Communication Technology, the frequency of cyber crimes is also increasing. With the ongoing advancement of technology, varieties of cyber crimes are taking place. New categories of cyber crimes from email hacking to software piracy, from cyber stalking to cyber terrorism are taking place in the qualified world of information and communication technology. The issues discussed in the various cases by the courts in India demarcates the fact that the Indian law on Information Technology is not robust and the doubts left in the provisions are reason for the escape of the accused.

The Information Technology Act is objectifying the promotion of electronic transactions rather than prevention of cyber misuse. It was only in year 2008 when the Amendment Act of 2008 has brought few specific categories of cyber crimes. The law on cyber crime needs to be strong in order to prevent future cyber crime. Law should change its recourse to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy. Though India has taken a lot of steps to stop cyber crime but the cyber law cannot afford to be static, it has to change with the changing times.

SUGGESTION

There are some basic precautions everyone using the Internet should take to protect themselves from the gamut of cybercrimes out there:

1. Use a full-service Internet security suite such as Norton Security Premium to ensure that you are protecting yourself against viruses, as well as other emerging threats on the Internet.
2. Use strong passwords, don't repeat your passwords on different sites and make sure to change your passwords regularly. A password management application can help you to keep your passwords locked down.
3. Keep all your software updated. This is most important with your operating systems and Internet security suites. Hackers are most likely to use known exploits in your software to gain access to your system. Patching those exploits makes it far less likely that you're going to be a victim.
4. Manage your social media settings to keep most of your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share with the broader world, the better.



5. Secure your home network with a strong encryption password as well as a VPN. A VPN will encrypt all traffic leaving your devices until it arrives at its destination. Even if a hacker manages to get in your communication line, they won't intercept anything but encrypted traffic.
6. Talk to your children about acceptable use of the Internet without shutting down communication channels. Make sure they know that they can come to you in the event that they're experiencing any kind of online harassment, bullying or stalking.
7. Keep up to date on major security breaches. If you have an account on a site that's been impacted by a security breach, find out what the hackers know and change your password immediately.



FIGHTING CYBER CRIME: PREVENTION AND PROTECTION

Ms. Bhagavath Harini V. J.,

*I B.A.LL.B. (Hons), School of Law, Sathyabama Institute of Science and Technology,
Chennai, Tamil Nadu*

I. Introduction:

Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. Two of the most common ways this is done is through phishing and pharming¹. Both of these methods lure users to fake websites (that appear to be legitimate), where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity. For this reason, it is smart to always check the URL or Web address of a site to make sure it is legitimate before entering your personal information.

Because cybercrime covers such a broad scope of criminal activity, the examples above are only a few of the thousands of crimes that are considered cybercrimes. While computers and the Internet have made our lives easier in many ways, it is unfortunate that people also use these technologies to take advantage of others. Therefore, it is smart to protect yourself by using antivirus and spyware blocking software and being careful where you enter your personal information.

II. History & Causes of Cyber Crime:

When computers and networks came into being in the 1990s, hacking was done basically to get more information about the systems. Hackers even competed against one another to win the tag of the best hacker. As a result, many networks were affected; right from the military to commercial organizations. Initially, these hacking attempts were brushed off as mere nuisance as they did not pose a long-term threat. However, with malicious software becoming ubiquitous during the same period, hacking started making networks and systems slow. As hackers became more skilful, they started using their knowledge and expertise to gain benefit by exploiting and victimizing others.

Wherever the rate of return on investment is high and the risk is low, you are bound to find people willing to take advantage of the situation. This is exactly what happens in cyber crime. Accessing sensitive information and data and using it means a rich harvest of returns and catching such criminals is difficult. Hence, this has led to a rise in cyber crime across the world².



III. Different Types of Cyber Crime:

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

1. **Hacking:** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.
2. **Theft:** This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.
3. **Cyber Stalking:** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.
4. **Identity Theft:** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.
5. **Malicious Software:** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
6. **Child soliciting and Abuse:** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting³.

IV. Categories of Cyber Crime:

Cyber crimes are broadly categorized into three categories, namely crime against

- Individual
- Property
- Government



Each category can use a variety of methods and the methods used vary from one criminal to another.

1. **Individual:** This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and “grooming”. Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

2. **Property:** Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person’s bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization’s website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

3. **Government:** Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations⁴.

V. **Cyber Crime in accordance with law⁵:**

Main Cyber Crimes

- Illegal access System interference
- Illegal interceptions Misuse of devices
- Data interference Computer related forgery etc

Misuse of Information Technology

- Unauthorised access/hacking
- Virus and worm-Attack/Trojan Attack
- E-mail and IRC related crimes
- Forgery
- Cyber stalking
- Breach of privacy and confidentiality

Key features of I T Act 200

- Electronic Documents can be signed with Digital signature and is recognized as equivalent to physical signature (sec 3 & 5)
- Electronic Documents are recognized as equivalent to paper Documents (sec 4)

Exceptions

- Bill of exchange promissory note, power of Attorney. Trust Deed, etc.
- Several Contraventions and offences are recognized under chapter IX & XII of the Act



- Extra territorial Jurisdiction covered
- Quick Justice

Offence Sections under IT Act 2000

- Tampering with Computer Source Documents (sec 65)
- Hacking with Computer Systems (sec 66)
- Publishing false Digital signature (sec 73)
- Breach of Confidentiality & privacy

Computer related Crimes covered under IPC and special Laws

- Sending threat messages through e-mail (sec 503)
- Forgery of Electronic records (sec 463 Ipc)
- E-mail spoofing (sec 463 Ipc)
- Web Jacking (sec 383 Ipc)
- Online sale of Drugs (Narcotic & Drugs prevention Acts)

VI. Prevention and protection:

1. Stay Updated

One of the easiest things you can do is keep your operating system and browser updated. For instance, the WannaCry ransomware exploited a flaw in Windows. Installing security patches helps protect you from these flaws. Luckily, Windows and most browsers have settings to update automatically, so you don't have to do anything other than stay protected.

2. Use Strong, Unique Passwords

Cybercrime prevention starts with using strong passwords. According to a report by Verizon, 63% of data breaches were the result of weak or stolen passwords. Just by using stronger passwords, many breaches could be prevented. It's also important to use unique passwords on every site and avoid social login to prevent hackers from getting your login information once and using it everywhere.

Consider using password managers to help you keep track of your passwords. You can also use special techniques, such as a password made from the first or second letter of every word in a sentence.

3. Always Use an Updated Antivirus

Your antivirus is only as good as its last virus definition update. Antivirus has to update often to protect you from current threats. With cybercrime on the rise, new threats emerge daily. Allow your antivirus to automatically update both the core program and virus definitions⁶.

4. Lock Down Windows

Windows has built-in security features, such as requiring a password to access a locked computer. You should always lock your computer when it's not in use, especially in public. Remember to use a strong password for your computer to prevent unauthorized access.

5. Look for HTTPS



Always look for HTTPS in the address bar of your browser when visiting any sites where you'll provide personal or financial details, such as shopping and banking sites. This identifies that the website is using a security certificate that encrypts the data sent between you and the site.

Most browsers provide details on a site's security certificate to help you determine if a site's legitimate or not. Taking those few extra seconds is just one way to take charge of cybercrime prevention.

6. Avoid Public Wi-Fi

Public Wi-Fi is a playground for hackers. Most data isn't encrypted, so it's easy to pick up credentials as you log in to email, social media, and banking sites. For best results, avoid using public Wi-Fi or use a VPN to protect your data.

7. Skip Emails and Texts You Don't Recognize

Phishing emails, texts, and social media posts are easy to avoid. If something seems odd or you don't recognize the sender, delete or avoid it. Sadly, 30% of phishing emails get opened, leading to identity theft, malware, and ransomware. Cybercrime prevention means avoiding any messages you don't trust.

If you receive a message from a site you use that tells you that something's wrong with your account, don't click the link in the email. Instead, exit the email and visit the website directly via your browser. If you can't find any issues, contact customer service to explain the email. It's safer and prevents many phishing scams from succeeding⁷.

8. Limit Online Sharing

Cybercriminals can learn intimate details about your life simply by how much you share on social media. They can figure out your passwords, especially those that use important dates or family and pet names in them. They know what sites and apps you use. For best results, limit your sharing. Set your social media profiles to private so only your friends see what you post.

9. Check the Site You're Shopping On

While you might feel safer on major websites, such as Amazon, it's a good idea to protect yourself by looking for warning signs on any site you shop on. Scammers may lure you in only to steal your information. Some signs to watch for include:

- Numerous grammatical mistakes
- Currency listed strangely, such as 100\$ versus \$100
- Extremely low prices – if it's too good to be true, it probably is
- URLs with hyphens and symbols, such as shop-here-low-prices.com
- No privacy policy
- No HTTPS

If anything feels suspicious, leave the site immediately⁸.

10. Always Monitor Your Accounts



Cybercrime prevention techniques aren't always perfect, but you can limit the damage by monitoring your accounts. Even when you protect yourself, the sites you use may still experience a breach. Keep an eye on your credit card and bank statements and check your credit report.

If you do spot strange activity, contact your bank or credit card company immediately. They can put a hold on your account to prevent any further charges and may even refund unauthorized charges.

11. Never Provide More Details Than Necessary

Some websites ask for your entire life history. Most of this is just for marketing purposes. However, you don't know what the site might do with that information. The only details you should ever need to provide while shopping online is your payment details and your shipping address⁹.

Be wary of any sites that ask you for additional personal details, such as your social security number. Basically, if you don't think a site needs certain information, skip it. If it's required and you don't feel comfortable providing it, move on to another website.

12. Be Careful About Downloading

A common scam is to scare you into downloading an app via a pop-up that says something is wrong with your computer or you need antivirus right now. One of the best cybercrime prevention tips to remember is to never download anything you don't trust. This includes attachments in emails and texts. If you're not expecting an attachment, contact the sender to see if they really did send it or not¹⁰.



Figure 1: Elements to protect from cyber crime



VII. Conclusion:

Though not all people are victims to cyber crimes, they are still at risk. Crimes by computer vary, and they don't always occur behind the computer, but they executed by computer. The hacker's identity is ranged between 12 years young to 67years old. The hacker could live three continents away from its victim, and they wouldn't even know they were being hacked. Crimes done behind the computer are the 21st century's problem. With the technology increasing, criminals don't have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren't guns anymore; they attack with mouse cursors and passwords.

END NOTES:

- [1] <https://www.techopedia.com/>
- [2] <http://www.crossdomainsolutions.com/cyber-crime/>
- [3] <https://searchsecurity.techtarget.com/definition/cybercrime>
- [4] <https://www.digitalcare.org/cybercrime-prevention-tips/>
- [5] <https://www.civilserviceindia.com/current-affairs/articles/types-and-prevention-of-cyber-crime.html>
- [6] Nalini R , ISBN No: 978-81-928510-1-3
- [7] Hemraj Saini, Yerra Shankar Rao, T.C.Panda , "Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications (IJERA)
- [8] Laila Dahabiyeh, "Networks of Cybercrime Prevention: A Process Study of the Credit Card", Twenty-Third European Conference on Information Systems (ECIS), Münster, Germany, 2015
- [9] Alpna, Dr. Sona Malhotra, "Cyber Crime-Its Types, Analysis and Prevention Techniques", International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 5, May 2016 ISSN: 2277 128X
- [10] Vineet Kandpal, "Latest Face of Cybercrime and Its Prevention In India" Article in International Journal of Sciences: Basic and Applied Research (IJSBAR) · January 2013



THE THREE ORGANS OF CYBERSPACE

Sunidhi Hegde

Student, Bangalore Institute of Legal Studies, Karnataka.

INTRODUCTION

The growth of Internet is nothing short of sheer genius which makes it a miracle of the century. The combination of mathematics, logic, and computer languages developing from scratch is a work that is worthy of high praise. Bright minds that worked hard back in the day have led us to lead a life of comfort and entertainment. The very first email is believed to be 'qwertyuiop'. Today we can share photographs, videos, even money in the form of Cryptocurrency and possibly in the future, the development of Artificial Intelligence. With these wonderful additions to our lives, there have also been some ugly facets of the Internet like pornography, phishing, hacking, fraud, etc. A new branch of crime has grown along with the Internet – Cyber Crime. Where crime is, the law follows to protect. Cyber Law is roughly defined as the law of information technology governing digital dissemination of information and software, information security and electronic commerce.

A BRIEF HISTORY

The Internet is a medium of communication that consists of interconnected computer systems using the Internet Protocol Suite (TCP/IP) that links systems all over the world. The Internet began as a small circuit of connection in four main places – at the Network Measurement Center at the University of California, Los Angeles (UCLA), the NLS System at SRI International, Menlo Park, the Culler Fried Interactive Mathematical Center at the University of California, Santa Barbara, and the Graphics Department of the University of Utah. This began in 1969 and was called the ARPANET, under the Advanced Research Projects Agency (ARPA).¹ By 1981, the ARPANET had established 200 nodes all over the United States of America. Subsequently, the ARPANET standardized using TCP/IP to transmit data packets across the network and the introduction of Domain Name System (DNS) was done. By 1990, researchers at the CERN (The European Organization for Nuclear Research) along with Tim Berners-Lee develop the World Wide Web, the HTTP (Hypertext Transfer Protocol), and the HTML (Hypertext Markup Language).² This opened up avenues for the general public to access the internet and establish contacts with several others like them across nations and led to the commercialisation of the Internet. By 2000, the USA had produced two-thirds of the most visited websites.³

¹ Gregory Gromov, *Roads and Crossroads of the Internet History*, http://www.netvalley.com/cgi-bin/intval/net_history.pl?chapter=1, (last visited on 31st October, 2018).

² Raphael Cohen-Almagor, *Internet History*, 2(2) INTERNATIONAL JOURNAL OF TECHNOETHICS 45, 53 (April – June 2011).

³ *Ibid*, at p. 56.



One of the first crises online was the introduction of a worm in 1988 by Robert Tappan Morris, who claims the damage caused was unintentional. What seemed to be a critical error turned a harmless program into a virulent denial of service which exploited known vulnerabilities like weak passwords in certain computer programs and emails.¹ In nearly fifteen hours, two thousand computers had been affected. About USD 100,000 - 10,000,000 worth damage was caused. The District Court and the Court of Appeal held Morris guilty.² The Morris case is considered one of the important judgments in Cyber Law. The courts heavily relied upon the then fairly new enactment called the Computer Fraud and Abuse Act, 1984. The Congress faced great difficulty in legislating on computer related crimes. In the 90s, there was a significant amount of development in harmonizing cyber laws in both developed and developing nations through international covenants. They aimed at data protection and privacy, protection of intellectual property, safe e-commerce and e-transactions and reducing cybercrime.³

With the assistance of the United Nations Development Programme, the National Informatics Center was set up under the Department of Electronics. By 1995, India had started the usage of the Internet and in 2000 the Information Technology Act was passed in accordance with the UN Resolution on Model Law on Electronic Commerce by the UNCITRAL (United Nations Commission on International Trade). Its objective is "to provide 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, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

CYBERSPACE AND CYBER SOVEREIGNTY

Little did science fiction writer William Gibson know that a certain word from his 1982 short story, *Burning Chrome*, would gain prominence and would be commonly used all over the world. He writes about two freelance hackers who fall in love with the same woman and attempt to hack into the systems of Chrome, a criminal indulging in cybercrime only to find that the woman they love was in ties with Chrome and has to leave town leaving the both of them devastated. He uses the word Cyberspace in the story with reference to a certain system, called

¹BOB PAGE, A REPORT ON THE INTERNET WORM, Computer Science Department, University of Lowell (7th November, 1988), <https://www.ee.ryerson.ca/~elf/hack/iworm.html> (last visited 31st October, 2018).

²USA v. Morris, 928 F.2D 504.

³Abha Chauhan, *Evolution and Development of Cyber Law - A Study with Special Reference to India* (January 2, 2013), <https://ssrn.com/abstract=2195557>, (last visited on 31st October, 2018).



'the Cyberspace Seven'¹ that one of the protagonists had built as a technology that let the people experience Internet internally, somewhat like an intermediate between Artificial Intelligence and hive mind. In the modern days, Cyberspace is the notional environment of the Internet, used synonymously with it.

However, the term Cyber Sovereignty does not seem to have been coined by any single person rather seems to have been in use generally. The word 'sovereignty' sees its origin in the Latin word 'supranus' which means supreme. Jean Bodin, a popular French used the word 'souverain' in his book, *The Republic*, published in 1576 which he describes as: "*Majestas est summa in cives ac subditos legibusque solute potestas*", which translates to the absolute and perpetual power within a State.² In the context of International Law, the Westphalian form of sovereignty is of great importance. It states that every nation-state has sovereignty over its territory and domestic affairs and follows the principle of non-interference in the affairs of another nation-state.³

INTERCONNECTEDNESS OF CYBERSPACE AND CYBER SOVEREIGNTY

It has been observed that the same cannot be followed strictly in cyber law. The borders are hazy in the virtual world which makes it all the more important to understand how Cyber Sovereignty is to exist and function to ease our lives. The Internet can be highly anonymous while also providing connectivity to very remote parts of the world. It is imperative for both the government and the governed to comprehend the scope of Cyberspace. While seeming to be a common ground for civil and economic discourse, it can be battlefield for waging wars.

In Cyber Sovereignty Workshop Series conducted by the U.S. Army War College, Pennsylvania the discussions were surrounded by three main agendas – policy making, strategies in implementing them, and theory and operations.⁴ Policy making, the responsibility of the legislative body is no easy task. In the absence of a policy, what the gaps and vulnerabilities that we are exposed to is to be understood. Following which, we understand what responsibilities follow the bridging of these gaps and how to address them. In the said discussion, it was proposed there exists an obstacle in closing the gaps which is the lack of a standard cyberspace lexicon. When certain terms are used by the official bodies, they are so due to the legal implications they carry while the public and the media uses the same terms in very vague terms. The vulnerability is caused mainly by the lack of situational awareness of victims.

The governmental agencies are responsible for protecting the rights of the citizens but it is not simple to identify the responsibilities given the expanse of the Cyberspace. This brings us back

¹WILLIAM GIBSON, *Burning Chrome*, http://project.cyberpunk.ru/lib/burning_chrome/ (last visited 31st October, 2018).

²S.R. MYNENI, *POLITICAL SCIENCE* 101 (2016).

³The Peace of Westphalia and Sovereignty, ER SERVICES, <https://courses.lumenlearning.com/suny-hccc-worldhistory/chapter/the-peace-of-westphalia-and-sovereignty/> (last visited 31st October, 2018)

⁴CYNTHIA E. AYERS, *RETHINKING SOVEREIGNTY IN THE CONTEXT OF CYBERSPACE – THE CYBER SOVEREIGNTY WORKSHOP SERIES*, US Army War College (Dr. Jeffrey L. Gogh et al. eds., 10-12th February, 2015).



to the question of whether Cyber Sovereignty really exists. It is believed that the Cyberspace should be free, the way it was meant to be but it cannot be ignored that the State is obligated to perform its duties. The key reasons why the Cyberspace cannot be mutually exclusive from the Government are–

- a) Cyberspace as an entity needs maintenance. It requires a terrestrial, physical maintenance unit, without which it won't exist. Since its users are physical and real, it's only fitting that it would be governed by people who are capable of maintaining, governing, and developing it, which is best done by an entity authorised to do so.
- b) Cyberspace now harbours economic discourse, which requires governing laws lest we want chaos in financial transactions.
- c) The information that we retain, send, and receive online is of significance to the physical in some way or the other.
- d) The connectivity that the Internet provides has also attracted the interest of official governmental activity to be online. Classified data is stored and shared over the web. It is a matter of national security to protect sensitive data.¹

JURISDICTION

One of the most intriguing aspects of Cyber Law is the determination of jurisdiction. Jurisdiction is considered to be of three types – (i) jurisdiction to prescribe, (ii) jurisdiction to enforce, and (iii) jurisdiction to adjudicate. These principles are based on –(i) subjective territoriality, (ii) objective territoriality, (iii) nationality, (iv) protective principle, (v) passive nationality, and (vi) universality.²

This paper will focus on personal jurisdiction of courts. The basis for this jurisdiction is usually physical presence in the territory. However, the landmark case of *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme (LICRA) and L'Union des Etudiants Juifs de France (UEJF)*³ holds a different view. Yahoo, with its headquarters in the USA filed for a declaratory judgment against the interim orders by the French Court in accordance with the First Amendment of the US Constitution. The District Court held that the French Courts were well within rights to exercise their personal jurisdiction and that enforcement of the First Amendment can be done only on the American soil.

¹Patrick W. Franzese, Lt. Co., *Cyber Sovereignty: Can it exist?*, 64 A.F. L. Rev. 1, 12-13 (2009) (discussing the key reasons of how cyberspace cannot be immune from cyber sovereignty).

² Tushar Kanti Saha, *Cyberspace – Conflicting Jurisdictional Spheres of Litigating IPR Claims*, 15 Journal of Intellectual Property Rights 364, 365 (September 2010).

³145 F. Supp. 2d 1168 (2001).



In *International Shoe v. Washington*,¹ the US Supreme Court adopted a three prong test for determination of minimum contacts for out-of-state defendants – (1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws;(2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and(3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e. it must be reasonable.

In *PresKap, Inc. v. System One, Direct Access, Inc.*,² the court found that a contract with an out-of-state party alone could not establish jurisdiction. The Florida Appeals Court held that electronic contacts with a computer database located in the forum state were insufficient to establish personal jurisdiction and warned about the unfairness of allowing jurisdiction where only contacts are between computers.

*Inset Systems Inc. v. Instruction Set Inc.*³ has an interesting holding. A case of trademark infringement where alleged infringement involved the Massachusetts defendant's use of the word Inset in its Internet domain name and in a toll-free numbers, both of which advertised the defendant's services. It was held that advertising over the Internet confers jurisdiction in any state or country where it could be accessed. The Court found that advertising on the web is enough to suggest that the defendant is purposefully availing the forum and could reasonably anticipate being hauled into court there.

The Information Technology Act, 2008 governs the jurisdiction related to Cyber Law in India. Indian Penal Code confers jurisdiction by applying to offences committed by persons outside of India targeting a computer resource located in India.⁴ The IT Act, 2008 in Section 75 confers jurisdiction to India of adjudicating matters against persons committing offences in India irrespective of their nationality.

CYBERCRIME AND ITS INVESTIGATION

Where there is opportunity to make it to the top easier, they are usually unethical and illegal.

The first international treaty on computer was the European Convention on Cyber Crime on the 8th of November 2001. The objectives of the convention were to harmonise domestic substantive laws of offences related to cybercrime and to harmonise investigation and prosecution of such offences. Cybercrime has been classified under white collar crimes. The offences are committed when there is presence of a computer system and a network. It can be defined as “offences that are committed against individuals or groups of individuals with a criminal motive to

¹ 326 U.S. 310.

² 636 So. 2d 1351 (Fla. Dist. Ct. App. 1994).

³ 937 F. Supp 161 (D. Conn 1996).

⁴ § 4, The Indian Penal Code, 1860.



intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).”¹

The categories which it can be divided under are –

- (1) Content related crime, i.e., child pornography, defamation, and criminal copyright infringement.
- (2) Traditional crimes using computers, i.e., cheating, forgery, etc.
- (3) Attacks on computer systems, like hacking. It is also called e-crime or hi-tech crime.²

Some of the most common offences are hacking, BOTS(a program installed in a system which allows the attacker to remotely control the targeted computer through a communication channel), key loggers(a software program or a device designed to secretly monitor keystrokes), website defacement(altering of a website by breaking into the web server), malware(a virus), phishing(masquerading as a trustworthy source to extract sensitive information such as passwords, bank account details, etc.), identity theft(impersonation by creating false profiles and false e-mail; identities in order to commit credit card faults, etc.).³

Under the Information Technology Act, 2008, several provisions cover the offences relating to computer systems. Fraudulent damaging of computer systems by means of tampering, destroying, deleting information attracts a fine extending up to five lakh rupees, imprisonment of up to three years or with both.⁴ Sending offensive messages of menacing character in order to cause annoyance, inconvenience, danger, obstruction, insult and injury through electronic means in such manners as to deceive the addressee of the recipient’s location is punishable with fine and imprisonment of three years.⁵ Deception by identity theft, violation of privacy, and cheating by impersonation also attract a three-year imprisonment. Publishing and transmission of sexually explicit acts⁶ or inducing children to be in an online relationship and coercing them in to sexually explicit acts⁷ is punishable for a term of five years on first conviction with a fine which may go up to ten lakh rupees. Further convictions may extend to seven years of imprisonment.

¹DEBARATI HALDER & K. JAISHANKAR, CYBER CRIME AND VICTIMIZATION OF WOMEN: LAWS, RIGHTS AND REGULATIONS (2011), ISBN 978-1-60960-830-9.

²APARNA VISHWANATHAN, CYBER LAW – INDIAN & INTERNATIONAL PERSPECTIVES ON KEY TOPICS INCLUDING DATA SECURITY, E-COMMERCE, CLOUD COMPUTING AND CYBER CRIMES 89 (2012), ISBN 978-81-8038-739-5.

³*Ibid*, at p.90.

⁴§ 65, The Information Technology Act, 2008.

⁵§ 66, The Information Technology Act, 2008.

⁶§ 67A, The Information Technology Act, 2008.

⁷§ 67B, The Information Technology Act, 2008.



INVESTIGATION

The investigation of such offences can be done only by a police officer of the rank of Inspector and above.¹ The offences being cognizable, a police officer of the specified rank, an officer of the Central or the State Government may enter any public space and search and arrest without a warrant any person who is of reasonable suspicion of having committed or of committing offences under the said Act.²

LAWS OF PRIVACY

George Orwell's book 1984 is a well-known work on totalitarianism. The Party constantly monitors what the people from the Outer Party do, through telescreens. The Thought Police taps into individual screens at any given point of time as a part of random checks. Every action and reaction is closely watched by the Thought Police. Free thought is condemned as Thought Crime. Free speech does not exist; the vocabulary is highly restricted in such a manner that propagation of agendas other than the Party's cannot be done. The dictionary is one where the vocabulary is constantly been shrunk down. Art and literature are nearly forbidden. The news is manipulated; nobody is sure what was true and what isn't. The book describes various possibilities of how a government can monitor our lives. The popular belief is that through the Internet, the government is at ease to do the same. All our searches are stored in our computer systems and in the databases of the services that we use online. We leave a digital footprint in whatever we do using electronic media.³

Privacy, hence, becomes an important aspect of democracy. One of the basic tenets of democracy is freedom. The government has no business in what we may do in our private lives. It does not govern our ideas, our religious beliefs, our thoughts and expression of the same. We are free to travel, to reside, to practice our faith, to choose our work, to be treated equally, to speak our minds. It is our Fundamental Right conferred by the Part III of the Indian Constitution. The Universal Declaration of Human Rights states that no one shall be subject to arbitrary interference with his privacy, family, and home and that each person is entitled to be protected against such interferences or attacks.⁴

THE RIGHT TO PRIVACY AS UNDER ARTICLE 21

The concept of privacy as a Constitutional right evolved in the 1950s, mainly in the context of police surveillance and domiciliary visits to the accused or the suspect's home. In *Kharak Singh v.*

¹§ 78, The Information Technology Act, 2008.

²§ 80, The Information Technology Act, 2008.

³GEORGE ORWELL, 1984, ISBN 978-81-929109-0-1.

⁴ Article 17, the Universal Declaration of Human Rights, 1948.



State of UP,¹ the petitioner alleged that the police subjected him to domiciliary visits to his home at any given point of time, the police surveillance, he contended was in violation of Article 21 of the Constitution of India. The police visits were held unconstitutional for infringing on the freedom of right to life. The Supreme Court had held that the right to life included privacy in his house. It was a landmark judgment to have included privacy within the ambit of right to life and laid the foundation stone to the development of privacy law in India.

The IT Act of 2008 defines personal information as any sensitive data like passwords, sexual orientation, financial information such as details of credit cards, bank accounts, PAN card, Aadhaar card, history of medical records, mental and physical health, and biometric data. People may not disclose personal information violating agreements, lest they wish to be imprisoned for three years.² Body corporates must handle sensitive data with reasonable security practices or pay for compensation.³

The fairly recent case of *Justice K.S. Puttaswamy v. Union of India*⁴ confers an explicit right to privacy within the ambit of Article 21 of the Constitution of India, 1950. Although the judgment does not explicitly mention the impact it might have on Cyber Law, it was still a landmark judgment given it was out around the time the Aadhaar case was *sub judice*. The present judgment shed some clarity on how the government must respect the privacy of the citizen. It set a precedent to the subsequent Aadhaar judgment, making it stronger.

The Aadhaar, previously named as the UID project (Unique Identification) under the UPA government, provides a unique identification to the residents of India. It included storage of biometric data of the huge Indian population, not so easy a feat. Its objective was to prevent duplicate and fake identities and to establish a robust, easy, and a cost-effective method of verification and authentication. With the enactment of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, several service providers began making it for Aadhaar details to be attached for availing the services. Mobile service providers, banks, LPG agencies made it mandatory for Aadhaar Number to be attached. This caused a furore among the public as this would allow the government to watch the activities of the citizens, which would fail the principles of democracy.

Retired Justice K.S. Puttaswamy filed a petition before the Supreme Court challenging the validity of Aadhaar. While the bench opined that Aadhaar would not make India a surveillance state, it suggested some back doors to prevent the same from happening. The bench raised concerns of data misuse. The judgment held it valid for linking Aadhaar for availing government subsidies and PAN card, while also ruling that children within the ages of 6 and 14 need not

¹ AIR 1963 SC 1295.

² §72A, The Information Technology Act, 2008.

³ § 43A, The Information Technology Act, 2008.

⁴ (2017) 10 SC 1.



require Aadhaar to avail schemes under the Sarv Shiksha Abhiyan. The verdict made it unconstitutional for mobile connections and bank accounts for making it mandatory to do so. It was ruled that bodies like the CBSE, NEET, UGC could not make Aadhaar Number to be linked for school admissions and exam registration.¹

CYBER PSYCHOLOGY

The Cyberspace has allowed us to stay connected with our friends, family and potential clients. It allows for a social discourse through the leisurely activities available to us like gaming and social media. It allows for us to express our thoughts freely and lets us know the same about several others who may be like minded. It facilitates growth of an individual by providing options for expanding our knowledge through easily accessible information. After the growth of Operating Systems like Windows and Apple, computers came to occupy spaces in our houses. Interaction with human beings has changed from sending emails to even dating people we meet online. Cyber Psychology is an attempt into studying the psyche of human beings when they enter into the Cyberspace as opposed to their real lives.

People often view the Cyberspace as an extension of their daily lives, a space where they are free to express their views and thoughts that lets them create an image of their own. In a way, the Internet is truly serving its purpose where people have free will. In psychoanalytical terms, the Cyberspace gives us the room to experience and exhibit part of our self that we may not be able to portray in our real life.² People can also shape the way they experience this realm, they can choose to alter it the way they wish to.

MEME – A SOURCE OF ENTERTAINMENT OR A MEDIUM OF PUBLIC OPINION

A meme is an idea, behaviour or style that spreads from person to person within a culture—often with the aim of conveying a particular phenomenon, theme, or meaning represented by the meme. Carlos Mauricio Castano Diaz says, “An Internet meme is a unit of information (idea, concept, or belief), which replicates by passing on via Internet in the shape of a hyperlink, video, image, or phrase. It can be passed on as an exact copy or can change and evolve. The replication can be by meaning, keeping the structure of the meme intact. The mutation occurs by chance, addition, or parody, and its form is not relevant. It depends both on a carrier and a social context where the transferor acts as a filter and besides what can be passed on. It can be interactive and some people relate them with creativity. Its role is to be known well enough to replicate within a group.”³ Memes are an excellent source of criticism of politics. Political ideologies like neo-nazism, right-wing extremism, Islamic extremism are constantly propagated

¹ 2018 SCC OnLine SC 1642.

² Azy Barak & John Suler, *Reflections on the Psychology and Social Science of Cyberspace*, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.334.7662&rep=rep1&type=pdf>.

³ CARLOS MAURICIO CASTANO DIAZ, DEFINING AND CHARACTERIZING THE CONCEPT OF INTERNET MEME, 6(2) Revista CES Psicología 82, 97 (2013).



through memes on platforms like 4chan and Reddit.¹ During the 2016 American Presidential Election, the conflict between republicans and democrats was perhaps best captured by memes. Right from the beginning of the Election, memers began documenting every event – from the conflict between Hillary Clinton and Bernie Sanders to the debates and campaigns.² In fact, the Trump campaign stems from an on-going joke about how the former industrial megalith and TV personality should become the head of the State.

Amidst rumours about the Russian intervention in the election leading to an unexpected result which crowned Donald Trump as the 45th President of the United States of America, word of the scandal of Facebook's data breach got out. The Cambridge Analytica, a British political consulting firm indulging in data analysis and data mining had used the data from Facebook without prior consent and had obtained user information of over 50 million people³ and had manipulated their viewer content and predicted and influenced ballot choices in a manner to further Donald Trump's campaign.⁴ This was revealed by an ex-Cambridge Analytica, Christopher Wylie. The Cambridge Analytica had been involved in yet another political event, the Brexit.⁵ This data breach would have had a direct on the creation and usage of the Election memes.

CONCLUSION

A popular show called the Black Mirror, which is an anthology, explores the possibilities of our future. In an episode called Hated in the Nation⁶, unpopular individuals die mysteriously in the most gruesome ways. This was the result of a game that eliminates individuals who are voted to be killed, which is unknown to the public. The antagonist is a former employee of Granular, a hi-tech corporate entity that created Automated Drone Insects for the purposes of pollination due to a sudden extinction of honeybees. A project backed by the government, the government uses the technology of facial recognition to keep tabs on the citizens, without their knowledge. The antagonist used the ADIs to kill the people. The major theme was how what we say online has real consequences on the person which we often neglect and indulge in unethical activities like

¹ Dark Net (Netflix broadcast Jan. 21, 2016).

² 2016 United States Presidential Elections, <https://knowyourmeme.com/memes/events/2016-united-states-presidential-election>.

³ Carole Cadwalldr & Emma Graham Harrison, *50 million Facebook profiles harvested for Cambridge Analytica in major data breach* (Mar. 17th, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (last visited 31st October, 2018).

⁴ Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions* (Mar. 17th, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> (last visited 31st October, 2018).

⁵ Carole Cadwalldr, *The Great British Brexit Robbery: how our democracy was hijacked* (May. 20th, 2017), <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexite-robbery-hijacked-democracy> (last visited 31st October, 2018).

⁶ Black Mirror (Netflix broadcast Oct. 21, 2016).



cyber bullying. The antagonist showed a karmic philosophy that we should be careful of what we say or we wish for, especially when we curse someone to death. The resultant of the masses hating collectively was not just the death of the most hated ones in the country but also of those who indulged in voting. In a blood-curdling climax, the episode ends with billions of ADIs travelling out in a swarm to complete their last task, to eliminate the voters. This particular episode, though fictional, carried heavy undertones of how people could use social media to create mass movements without fully fathoming the magnitude of it. The second message it carries is a caution that the government may turn into the Big Brother.

The Cyberspace has been occupied by the citizens, the government and the international community for decades.¹ The Cyberspace when used by the citizens falls into the wrong hands and gives rise to crime in the Internet. To protect the citizens from threats and dangers, the government comes to their rescue and helps with investigation of crime and prevention using legislation of Cyber Law. But the involvement of the government may have an adverse effect on the freedom of the Cyberspace and that of the citizens themselves. The press and the media have long been the modes of creation of public opinion and critics of the government, the social media has only recently joined them but the impact it has had on the socio-political front is far greater than its counterparts in their pasts.

¹HAO YELI, A THREE-PERSPECTIVE OF THE CYBER SOVEREIGNTY, 7(2) PRISM 109 (Dec. 21, 2017).



CHILD PORNOGRAPHY IN THE DIGITAL AGE: LEGAL CHALLENGES

Ms. Romita Reang,

Research Scholar,

Department of Law, North-Eastern Hill University, Shillong, Meghalaya.

1. Introduction

The easy accessibility of child pornography over internet has become a major social problem. It is very clear that this is a problem of international proportion and it gravely infringes on the child's right. Child ¹ pornography is a type of sexual exploitation and it has been the major child exploitation offence in the recent years. The proliferation of such material is further achieved through social media and technological developments in the internet connected world. The production and distribution of child pornography has become more extensive with the wide availability of digital technologies such as digital cameras, mobile phones, peer to peer file sharing, strong encryption, Internet anonymizers and cloud computing.² Thus, for law enforcement agency it has become very challenging to fight the proliferation and sharing of child abusive materials via internet.

Child pornography existed even before the advent of internet technologies. The roots of child pornography date back to ancient Greek civilization and the Romans were famously tolerant of pederasty. In the middle of the fifteenth century large-scale production of such offensive materials became possible with the invention of printing press. The true birth of child pornography occurred during the mid 1960s with an explosion in the production of sexually graphic photographs of children in Europe, Asia, Australia and North Africa. By the late 1960's and early 1970's child pornography was the basis of a major worldwide market. This development was partly the result of relaxation laws against child pornographic materials in many countries.³ It is undeniable that the Internet facilitated for the wide spread of child pornography and the creation of an expanding market for its consumption.

The increasing crime of sexual abuse and violation on children across the world is a global concern and this is mainly due to the alarming rate of the production, distribution and easy accessibility of child pornographic material on the internet. The main consumers are

¹ The definition of 'child' varies in different jurisdiction of world, according to Article- 1 of the Convention on the Rights of the Child (CRC), 1989 where a child means every human being below the age of eighteen years.

² Jasmine V. Eggstein & Kenneth J. Knapp, *Fighting Child Pornography: A Review of Legal and Technological Developments*, 9, 4, JDFSL.1, Article-3 (2014). DOI: <https://doi.org/10.15394/jdfsl.2014.1191> Available at: <https://commons.erau.edu/jdfsl/vol9/iss4/3>.

³ IAN O'DONNELL & CLAIRE MILNER, CHILD PORNOGRAPHY: CRIME, COMPUTERS AND SOCIETY, 3 (2012).



paedophiles¹, child pornographers² and sexually curious persons who simply fantasize about sexual activity with children. Paedophiles use such kind of materials for a variety of purposes ranging from private sexual use, trading with other paedophiles and grooming children for exploitation. Thus, it takes shape of a crime which operates beyond the boundaries of a particular country or state jurisdiction and leads to sexual exploitation of children worldwide. It also gives birth to a new pattern of globalised crime with increased incidences of child sex tourism, child rape, child trafficking. The problem is further compounded when the existing legislation cannot prevent such instances of risk to children. One of the barriers to attaining verifiable and accurate rates of internet child pornography is that most developing nations have no reporting infrastructure for ascertaining basic rates of internet child pornography and let alone capabilities to identify online sexual offenders. This creates statistical anomalies and a lack of concrete information as to the true extent of the problem. In India, The National Crime Records Bureau (NCRB) statistics do not provide any specific information on the child pornography cases. As a result the gravity of the issue is not being much understood.³

Child pornography law is a very recent development. There are many nations and international efforts to tackle the problem as now it is recognised as a specific form of child abuse. The volume is rampantly increasing particularly on the internet despite of unceasing efforts by the law enforcement agencies. The law has reacted to this situation by adapting its definitions, increasing sentences, providing new roles and powers to law enforcement bodies and service providers. Despite increase in global child protection laws many countries still do not consider child pornography a crime. There are still many countries around the world that do not have specific legislation on child pornography. According to the International Centre for Missing & Exploited Children (ICMEC) 53 countries still have no law and do not consider child pornography a crime. Criminal law is traditionally associated within country and policing is a core activity of nation states⁴. However, this activity is unsettled within a borderless medium such as the internet. The policing of internet child pornography are possible at a national level only when the perpetrators are within the jurisdiction of nation state or extra territorial policing activity is possible.

2. Defining Child Pornography

To fight against child pornography it is very important to define child pornography from a legal point of view. The European Union's Framework Decision on combating the sexual exploitation

¹ A person who has sexual attraction to children.

² A person who produces or publishes child pornography.

³ Crime in India Statistics 2016, Ministry of Home affairs, India, <http://www.ncrb.gov.in>CII2016>pdfs>NEWPDFs>

⁴ Artist Jeff Koons, *Despite increase in Global Child Protection Laws Many Countries still do not consider child pornography*, THE INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN, <https://www.icmec.org/press>.



of children and child pornography which entered into force in January 2004, required member countries to take necessary measures to comply with this framework decision. The Council Framework Decision defines child pornography as pornographic material that visually depicts or represents:¹

- (i) real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or
- (ii) A real person appearing to be a child involved or engaged in the conduct mentioned in (i).
- (iii) Realistic images of a non-existent child involved or engaged in the conduct mentioned in (i).

The Council of Europe's Cybercrime Convention 2001, which came into force on 1st July, 2004 defines child pornography under article 9(2) as pornographic material that visually depicts:²

- (a) a minor engaged in sexually explicit conduct;
- (b) a person appearing to be a minor engaged in sexually explicit conduct;
- (c) realistic images representing a minor engaged in sexually explicit conduct.

Finally, United Nation's Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, which came into force on 18 January 2002, defines child pornography in article 2(c) as "*any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child, the dominant characteristic of which is depiction for a sexual purpose*".³

All the three documents define a child as under the age of 18 years and cover both real depictions as well as realistic and simulated representations within the definition of child pornography. Computer generated images as well as images of real persons who appear to be a child under the age of 18 years would therefore come under these definitions.⁴

3. International Instrument

Many countries have bolstered their respective legislation or statutory codes to assertively prosecute and punish those offenders for the production, selling, sharing, and acquisition of child pornography. Currently, there are five widely accepted international instruments which address the issue of Internet child pornography at the international level:

- (1) The Convention on the Rights of the Child.
- (2) The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.
- (3) The U.N. Protocol to Prevent, Suppress, and Punish Trafficking in Persons.

¹ YAMAN AKDENIZ, INTERNET CHILD PORNOGRAPHY AND THE LAW: NATIONAL AND INTERNATIONAL RESPONSE, 10 (2008).

² *ibid*

³ *ibid*

⁴ *ibid*



(4) The Council of Europe Convention on Cybercrime.

(5) The Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse.

1. Convention on the Rights of the Child.

The United Nations Convention on the Rights of the Child (UNCRC) serves as the strong pillar of international covenants respecting the various human rights of children as a matter of International. 193 countries were signatory members and ratified this convention. Initially, Internet child pornography was not a recognized as a problem during the Convention's formation in 1989. Gradually, some provisions of the convention could be seen to relate to the core issues of Internet child pornography, the main purpose of the convention is targeted at fundamentally related to children's rights and protections. This convention monitors that the signatory countries works together effectively to recognize and protect some basic human rights for children.¹

2. Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.

In 2000, the United Nations adopted the Optional Protocol to the UNCRC because it was concerned about the new dangers posed to children by the emergence of the Internet. The Optional Protocol specifically identifies the issue of child pornography as one of its major concerns about the growing availability of child pornography on the Internet and other evolving technologies. The International Conference on Combating Child Pornography on the Internet was held calling for the worldwide criminalization of the production, distribution, exportation, transmission, importation, intentional possession and advertising of child pornography, and stressing the importance of closer cooperation and partnership between Governments and the Internet industry.²

4. U.N. Protocol to Prevent, Suppress, and Punish Trafficking in Persons.

This convention provides provisions for combating Internet child pornography although the Protocol does not specifically address the problem in detail. However, the Protocol is important for addressing and dealing with human trafficking and other related crimes. This protocol will invariably remain relevant and pertinent as a supporting structure for combating Internet child pornography.

5. Council of Europe Convention on Cybercrime.

The Council of Europe Convention on Cybercrime (2001) is one of the first instruments to harmonize standards for various facets of Internet crime, fraud, abuse, and illegality. The Convention is a more contemporary instrument that can be both flexibly and universally applied among nations, making it effective to both law enforcement and criminal judicial

¹ Alexander Kalim, *Addressing the Gap in International Instruments Governing Internet Child Pornography*, 437 *CommLaw Conspectus*. Vol. 21, (2013). Pg 437-444

² *ibid*



officers. Article 9 of the convention is dedicated to offences related to child pornography. The Council of Europe's Convention on Cybercrime is the first legally binding international instrument to establish universal standards regarding the criminalization of computerized child pornography, the Convention also takes an important step toward containing this offense on a global scale.¹

5. Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse.

This convention updates some of the provisions of the Convention on Cybercrime. The Convention directly addresses child pornography in particular and it remarks that child pornography constitutes sexual abuse. The Convention addresses sexual tourism an area uncovered by previous instruments and currently recognized as the universal standard. Notably, the Convention sought to harmonize the "best practices" of the member States.²

In 1999, in Geneva the Parties to the *International Labour Organization (ILO)* adopted the Convention on Prohibition and Immediate Action for the Elimination of the *Worst Forms of Child Labour Convention (WFCLC)* where child pornography also falls under its scope.³

4. Legislature and legal developments in India

The Indian Constitution already provides safeguards for the protection of child rights and has included fundamental rights like right to free and compulsory elementary education till the age group of 6-14 years,⁴ right to be protected from any hazardous employment till the age of 14 years,⁵ right to equality and right against discrimination in order to protect the interest of children. The Constitution also lays down Directive Principles of State Policy which reaffirm the policy of protection against exploitation and abuse of children at the tender age for economic necessities.

The Information Technology Act (Amendment) Act 2008 aims to make revolutionary changes in the existing Indian cyber law frame work. There are insertions of new express provisions to bring more cyber offences within the purview of the Information Technology Act, 2000. The amendment incorporated Section 67 A to 67 C to the parent Act.⁶ The production or viewing of child pornography in India is governed by the Information Technology (Amendment) Act, 2008

¹ ibid

² ibid

³ International Labour Organisation (ILO) No-182 Worst Forms of Child Labour Convention (WFCLC), this convention was adopted by International Labour Organisation to prohibit and eliminate all forms of sexual exploitation of children and recognizes the use, procuring or offering of child for production of pornography or for pornographic performance.

⁴ INDIA CONST, art 21.

⁵ INDIA CONST, art 24.

⁶ Nuzhat Khan & Nida Zainab Naqvi, Child Pornography In Digital Age And The Law In India- Analysis, eurasiareview news & analysis May , 3(2017) <https://www.eurasiareview.com>.



which makes the publication or transmission of such 'electronic' material depicting children in sexually explicit act, etc in electronic form is punishable with imprisonment and fine.

Section -67 B of Information Technology (Amendment) Act, 2008, lays down that -

“Whoever publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or 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 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 facilitates abusing children online or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children are also made punishable under the same legislation”.¹

The Indian penal code 1860, (IPC) seeks to redress the problem by making the sale, letting to hire, distribution, public exhibition, circulation, import, export and advertisement of obscene material is an offence, punishable with imprisonment and fine.² The Protection of Children from Sexual Offences Act, 2012 (POCSO) also recognizes child pornography as a crime and punishes it by severe prison sentence and fines, depending on the severity of the crime.³

In India, the effectiveness of available law on child pornography was tested in the case of *Avinish Bajaj v. State (NCT of Delhi)* 2008, High Court of Delhi. The law in the country is not adequate to meet the challenge of regulating the use of the internet to prevent dissemination of pornographic material. The court referred to the legislative response of other common law jurisdictions on this matter to seek better solutions.⁴ India may want to develop a different legislative model to regulate the use of the internet with a view to prohibiting its use for disseminating child pornography materials nevertheless the task deserves the utmost priority.

Realizing the gravity of such impact upon children, the Supreme Court of India held that the websites showing child pornography, especially of children between 14 to 18 years should be strictly banned and directed that concerned authorities should take positive steps immediately to stop the menace of child pornography. It gave directions to the Secretary of Department of Telecommunications (DoT) and other departments of Government of India to issue directions to call off sites showing pornography.⁵

¹ IT Act 2008 sec 67B.

² IPC sec 292 and 294.

³ POCSO ACT 2012 sec 13 and 14.

⁴ The High Court of Delhi decided in *Avinish Bajaj v. State NCT of Delhi*, (2008) 3 CompLJ 364 Del.(India) (also known as Baze.com case).

⁵ *Kamlesh v. Union of India and others*, (2014) 6 SCC 705 (India)



Since the incidence of Delhi gang rape of 2012, the movement against 'rising rape culture' in India made a significant progress to stop videos of sexual abuse being shared online. Following the hearing in Prajwala's case, the Supreme Court launched a special technical committee tasked with creating a mechanism for the mandatory reporting and blocking of online content of rape and child porn. Based on the recommendations of the committee, the Supreme Court further gave direction to the central government to finalize the Standard Operating Procedure (SOP) for handling Complaints involving child pornography by November, 2018.¹

5. The Internet and Advance Digital Technology

Types of violence and harms against children in cyberspace and in relation to new technologies include sexual abuse and commercial sexual exploitation including online grooming. Exposures to illegal and harmful materials that can cause psychological harm lead to physical harm or facilitate other detriment to a child. The midpoint of all this is the modern technology which is the ultimate distributor of child pornography material across the world. The concern is that most children are familiar with the use of technology and social networks which are rapidly becoming a way of life in the modern world. As a result, these days access to cyber-space and mobile phones by children have led to an increased risk and exposure to different information on the internet some of which are very destructive and promote sex trade and trafficking. Technology is used for communication purposes, but unfortunately this also facilitated to disseminate child pornography. The Internet and advances in digital technology have provided fertile ground for offenders to obtain, share, produce, advertise, and sell such materials.² The Internet has also allowed offenders to form online communities with global membership not only with the intention to facilitate the trading and collection of these images, but also to facilitate contact with each other and children and to create support networks among offenders.³

6. Role of Internet Service providers

The role and responsibility of Internet Service Providers (ISPs) in reporting and preventing child pornography materials through collaboration with other relevant professional is crucial to fight child pornography. The Supreme Court of India held that the websites showing child pornography, especially of children between 14 to 18 years should be strictly banned and directed that concerned authorities should take positive steps immediately to stop the menace of child pornography. It gave directions to the Secretary of Department of Telecommunications (DoT) and other departments of Government of India to issue directions to call off sites showing

¹ [http://www.livelaw.in/finalze-sop-for-handling-complaints-involving-child-pornography-by-15-november -sc-directs-centre-read-order](http://www.livelaw.in/finalze-sop-for-handling-complaints-involving-child-pornography-by-15-november-sc-directs-centre-read-order), by apporva mandhani , oct 22,2018 10:16 pm

² Richard Wortley, Stiphen Smallbone, *Child Pornography on the Internet*, Problem-Oriented Guides for Police, (2006) last updated May, 2012; available at: <http://www.cops.usdoj.gov/Publications/e04062000.pdf>.

³ MAX TAYLOR AND ETHEL QUAYLE, *CHILD PORNOGRAPHY: AN INTERNET CRIME*, (1st ed. 2003).



pornography.¹ Service providers (ISPs), mobile phone companies, Internet cafes and other state holders that could be indirectly involved with the dissemination of child abuse images should be held responsible to adopt child protection measures in relation to their business.²

Two mandatory measures to be adopted are:

- (i) The obligation to report child abuse content and the compulsory adoption of Code of Conducts.
- (ii) Corporate regulations.

There has been challenge in making practically possible these obligations legally binding and the vast majority of corporations that have eventually adopted a Code of Conduct to promote the safety of children using the Internet. Therefore there is urgent need to develop specific legislation to address reporting of alleged illegal materials. This includes signing of code of conduct, display and dissemination of useful information related to Internet safety and implementing good practices within the business operations to keep children protected. Moreover such acts have also helped in raising public awareness on the issue.³ The Internet service providers are further directed to block access to websites containing child abusive images through filters. To end the circulation of sexual abuse image and blocking the access to other content on the Internet is a very delicate and challenging issue. Moreover, Internet filters can be helpful only for websites and not for others like chats, file-sharing programs, blogs, and peer-to-peer networks.

7. Varied Definitions and Legal Framework

The problem of child pornography over internet is magnified by the presence of variable definitions in different countries along with various legal frameworks. The law is inconsistent across jurisdictions about what constitutes child pornography. For example, in some countries photographs of a naked child is considered production of child pornography, while in other countries one must prove that the motivation or intent for making the image was sexual. In some countries no actual child involvement is required to prosecute for offence of production or making of the pornography, when such is created artificially through computer techniques. In the countries with legal systems, to prosecute for production of abusive material it is very challenging where actual identification of the victim cannot be traced.

Even where there is a clear understanding of what constitutes child pornography within a country or region, the definition and age of a child under the law may be inconsistent. Different countries have different definitions of distribute abusive materials. In some countries the law states that distribution sits with the person who uploads an illegal image into cyberspace. In other countries, distribution takes place at the site of the computer hub, network or ISP. Still in

¹ Kamlesh v. Union of India and others, (2014) 6 SCC 705.

² Deborah Muir, *Violence against Children in Cyberspace*, ECPAT International, (Sep 2005) www.ecpat.net.

³ Deborah Muir, *Violence against Children in Cyberspace*, ECPAT International, (Sep 2005) www.ecpat.net.



other countries distribution is recorded at the physical location where an individual takes receipt of such material. It is also very difficult to investigate and prosecute possession of criminal material accessed in virtual settings than possession of such material in physical settings.¹

In some jurisdictions, only viewing without downloading such illegal material onto a hard drive is considered not an offence. In some countries, this action is known as an access crime and it carries a much lower sentence than actual possession. Another distinct feature of child pornography possession in virtual settings is the development of encryption software that allows an individual to possess illegal material in the belief that law enforcement may not be able to crack the encryption or obtain the key to decrypt the material. In some jurisdictions it is an offence to refuse to divulge the key for encryption software to police. But in many other countries this is not a crime in and of itself. The age of consent is another barrier before the law enforcement especially when the victim is post-pubescent. In most countries, governments have recognized an age at which a child can consent to sexual activity. The age may and often is not consistent with the age of consent recognized by the statutes depending upon where they exist and belonged. Therefore, a child might consent to have sexual relations with any person, depending on the jurisdiction, but a child cannot consent to have his or her picture taken during that legal sexual activity. This lacuna has led to statutory appeals which in some instances have resulted in the lowering of the age contained in the child pornography legislation.

8. Legal Challenges ²

The cybercrimes tend to present many challenges faced by law enforcement agencies for the investigations and joint operation. The worldwide application and globalised character of the Internet, which has either controlling agency nor has it a storage facility or allows for the emergence of new websites with child pornography content all the time even if at the same time others are being closed down. This means that the proliferation of the illegal content is unstoppable and for profit, personal gratification at the expense of victimizing children is extremely difficult to be closed. Additional challenge to the law enforcement can be the uncertainty around the jurisdiction responsible for investigating certain organizations or offenders. This is the reason why some pornography crimes on the Internet remain uninvestigated due to the uncertainty under which law enforcement jurisdiction fall. Unfortunately, in those cases when the host country of a certain child pornography website is unknown to the police teams, the investigation of the website is impossible. On the other hand, next to the peer-to-peer networks which facilitate the trade and exchange of child pornography

¹ Ibid pg 29

² Mihaela Astinova, *The Crime of Child Pornography: European Legislative and Police Cooperation Initiatives*, Tilburg University, Master Thesis (2013) pg-50-52.



images is that the offenders challenge the law enforcement with sophisticated servers which enable to hide the sender's identities from an email or hide which has been exchanged or traded by different methods. Looking critically on the purposes and use of the Internet, it is obvious that it has been invented to facilitate connection and access to information by people facing no geographical borders. Due to the international usage of the Internet, it has been difficult to be regulated and sometimes laws that may control its usage are missing. The reason most probably lies on the balance simultaneously to protect children on the one hand and to respect rights of freedoms of speech and private life. The varied legislations among countries also challenge the law enforcement. For instance many countries have different legal definitions of a child when it concerns child pornography some countries do not have specific legislation on the crime, or do not have provisions on computer facilitated offences. At a national level as well as internationally it can be stated that the major dilemma for the law enforcement authorities to investigate and destroy child pornography practices are very similar related to the discrepancies in the legislation, particularly to identify the age of the victim appearing in the material and to estimate the graveness of the picture and whether it falls under the definition of child pornography. It is obvious that materials showing explicit sexual abuse with children are considered child pornography.

At international level issues like the lack of material and human resources is considered to be quite inappropriate when we talk about fighting of child pornography. This is related to the better organization of the specialized units and improvement of communication between the law enforcement authorities, NGOs and industry. Nonetheless Europol and Interpol have a very solid database and mechanism for cooperation and sharing information techniques, a better relation with the national units is required. From a technological perspective the development of stronger international, national and local intelligence and investigative practices as well as sophisticated technological support should never stop evolving since the offenders techniques are getting more and more difficult to detect. Additionally, the bureaucracy in the mutual legal assistance procedures may also put at risk the effective investigation and cooperation among countries. Despite the difference in the statutory regulations, definitions and investigation practices, the law enforcement agencies and national authorities have made a huge progress in combating child pornography and exploitation of children. Through sharing data files, reporting channels, international sources, the police authorities can conduct high quality intelligence, track the initial places of child sexual abuse materials and prosecute their offenders. Unfortunately these steps take relatively long time and sometimes the abusive content is impossible to be removed which brings the dissemination process unstoppable.¹

¹ Deborah Muir, *Violence against Children in Cyberspace*, ECPAT International, (Sep 2005) www.ecpat.net.



9. Legal enforcement and Need for Reformation¹

Many unusual challenges confront legislatures, prosecutors and law enforcement agencies in their efforts to combat online grooming.

Firstly, notions of anonymity and the speed of interactions and relationship-forming, as compared with physical settings require that law enforcement agents act quickly. Even though the child may be physically situated far from the online groomer, a face-to-face encounter can still occur after just a few weeks of intense communication.

Secondly, groomers can join their efforts online to gain more information about their victims with searches of online databases, including phone books and profile searchers. Often victims of online grooming may not even realize that someone already had gathered personal information about them. Legislatures need therefore to draft comprehensive laws that prohibit the private sector from publishing personal details, particularly those of children.

Third, online grooming can be a much more private and secret interaction in cyberspace. If the groomer has their target mobile phone number, for example, they can easily communicate with the child from a distance, with no one ever seeing the two of them together. These private communications create an obstacle in the collection of evidence and prosecution of crimes. Laws are required to ensure that the private sector maintain records for a specified period of time, where possible. As well, pressure can be placed on mobile phone companies to provide educational resources when individuals, particularly young people, buy telephones and other ICT tools.

Finally, one person can groom several children at the same time. In addition, if a young person rejects their advances, they can disappear and adopt a new identity to re-approach the same child. Law enforcement needs to be trained on how to investigate the possibility of net safe.

It is pertinent for reformation of Nation States legislatures for effective functioning to combat the issue of Child pornography.²

a) Domestic Criminal Law: National governments are urged to devise and implement legislation and harmonize internal laws to protect children from all cyber crimes including exposure to illegal or inappropriate materials and all actions related to child pornography for creation, dissemination, accessing, downloading, possession and incitement. Governments must ensure that legislation on child pornography protects all children under the age of 18. A child under 18 should not be considered as able to consent to engagement in pornography, prostitution or trafficking. Internal and cross-border coordination of laws must include action to define child pornography explicitly within the law and to define and outlaw images of abuse created through virtual techniques.

¹ Ibid

² Deborah Muir, *Violence against Children in Cyberspace*, ECPAT International, (Sep 2005) www.ecpat.net.



b) Domestic Administrative Law: Recognising that ISPs offer a different service than traditional telecommunications businesses, governments are advised to formulate and implement laws and regulations specific to ISPs. In particular, laws are required to ensure ISPs remove or prevent accessibility to illegal material of which they have knowledge¹. Further, laws should require a minimum monitoring obligation on behalf of ISPs to prevent all actions associated with online child pornography.

c) Domestic Civil Law: In the absence of any legislation, either internationally or domestically, which holds the private sector accountable for violence committed against children it is very difficult for law enforcement to pressure businesses to cooperate fully in their investigations. As such, governments are urged to ensure laws exist, whether criminal or civil, to hold those accountable for acts of commission and omission responsible for harm committed against children as a result of their negligence. The money collected through fines or recovery or both may be used to assist survivors.

d) International Law: With the creation of the International Criminal Court, governments have access to another tribunal for trying crimes against children where particular offences have international implications. As such, governments are urged to classify the crime of being involved with child pornography as a crime against humanity thereby falling under the principle of universal jurisdiction.

e) Cross-Border Cooperation: Cross-border jurisdictional issues remain a barrier for achieving comprehensive solutions. World governments are urged to devise mechanisms for dealing with the cross-border jurisdictional matters.

The following components are encouraged to be included in any law enforcement strategy.

a) Putting the victim first: The child survivor welfare must be made the priority in investigations. A child protection must outweigh the prosecution of the offender. Within the judicial process, the victim's welfare must remain a priority. In giving evidence it should not be necessary for a court to examine every image in a collection to determine the guilt or innocence of an accused.²

b) Cooperation: Cooperation is required to facilitate the sharing of experience, lessons learned and good practices and to assist countries to adopt targeted legislation and law enforcement actions to better protect children. Greater efforts need to be made by law enforcement agencies to share investigation techniques and identification methods.

c) Encourage Specializations: Specialist police units charged with combating cyber related crimes are urgently required. These units need to be equipped with technological means and expertise, as well as staff conversant with children rights. Law enforcement agencies are urged to seek the collaboration of hotlines and ISPs in investigating cases and identifying future

¹ Ibid pg 38-39

² Deborah Muir, *Violence against Children in Cyberspace*, ECPAT International, (Sep 2005) www.ecpat.net.



challenges. In this context, units that hold databases of abuse images must establish and adhere to strict protocols and guidelines for their access and management.

10. Conclusion

The paper concludes that child pornography has some form of negative effects on children and recommends that legislations prohibiting child pornography should be implemented effectively. As cyberspace and online file sharing expands, a new generation of criminals has turned to their computers to assist in producing and concealing their illegal activities. The explosion of internet use in an ever-expanding globalized world will continue to have both unimagined positive social, economic, and human consequences in congruence with the negative side-effects associated with crime facilitation in a digital age. This study identifies specific challenges law enforcement agents may encounter in fighting Internet child pornography. Defining child pornography can be complicated by definitional challenges and identifying the age of children depicted in images. Child pornography crimes may involve multiple jurisdictions and cross national borders. Law enforcement agencies are urged to seek the collaboration of hotlines and ISPs in investigating cases and identifying future challenges. In this context, units that hold databases of abuse images must establish and adhere to strict protocols and guidelines for their access and management.



BALANCING OF INTERESTS AND THE CONCEPT OF RESPONSIBILITY SHARING VIS-À-

VIS CYBER CRIME

Trishna Gurung,

Research Scholar,

Department of Law, North-Eastern Hill University, Shillong, Meghalaya.

Introduction:

One of the greatest inventions of all times in the human memory has been the invention of the “internet”. With the passage of time and generations, the technological advancements are tracing a whole new world known as the “Cyber Space” in which our every action leaves a non-erasable imprint of our existence. The role of cyberspace has always been a tricky one and of debatable interest from every part of the global society. Factors like the unbeatable speed of connecting beyond global boundaries, the vast ocean of information accessible by all at a minimal cost have made the internet the most popular medium of communication, information, commerce and governance within a very short period of time. Similarly, the same factors equally provide scope for the commission of cyber crimes. The Government of India has enacted the Information Technology Act, 2000 (amended in 2008) with an aim to deal with this menace along with the National Policy on Cyber Security, 2013 and other legislations. However, the recent crime records speak of different reality. The question which arises here is “is legal control the only solution for checking this problem?” Thus, this paper attempts to briefly discuss the concept of cyber crime, its nature and pervasiveness and legal measures while highlighting the need for the balancing of interests and concept of responsibility sharing as a global community for regulating and minimizing cyber crimes.

Conceptual Analysis

Crime affects a large number of people either directly or indirectly. People suffer physical, emotional, sociological or financial injury or loss as a result of crime. Such crime affected persons are known as victims and they need prompt redress by easy access to justice. A crime may be in the form of traditional crimes, political offences, economic crimes, social crimes, all other remaining crimes or in the form of a new species of crime known as cyber crimes. The rapid advancement in the field of information technology during the last few decades have given rise to a new computer related crimes commonly known as cyber crimes. Cyber crimes are being committed at an alarming rate and in every walk of life. Numerous people are falling prey to it every second. In common parlance, the terms “cybercrimes” and “computer crimes” are usually used interchangeably. Dohn B. Parker¹ has distinguished between the two terminologies by giving the following definitions:

- i. Computer crime- A crime in which the perpetrator uses special knowledge about computer technology.

¹ A computer crime expert and a security expert with 30 years of experience in the field.



- ii. Cybercrime- A crime in which the perpetrator uses special knowledge of cyberspace.¹

In other words, cyber crime may be defined as any wrongful act in which a computer is used either as a medium or target of crime.

Cyberspace² is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks. The Black's Law Dictionary defines the term cyber space as "the realm where computer communications and simulations are used on the internet. It is like the human psyche translated to the internet. The objects are not physical and made up of data manipulation." The term was started by William Gibson in 1982.³

Cyber crime and legal measures- desired goals

With the internet becoming an indispensable aspect of our daily lives whether in the fields of education and research or e-governance or e-commerce or defence, the bi-polar role of cyber space cannot be ignored in anyways. As such, cyber threat seems like it is here to stay and would give rise to further complications in days to come unless a working mechanism for controlling or minimising the menace of cyber crime is formulated. In an attempt to achieve the said goal, the Indian Parliament enacted *the Information Technology Act, 2000* based on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) with an aim "to provide 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, to facilitate electronic filing of documents with the Government agencies".⁴ This Act brought about certain significant amendments in the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. The Act was amended in 2008 and called as the Information Technology (Amendment) Act, 2008 along with various rules.

Along with the Information Technology Act, 2000, the Government of India has been taking steps towards formulating mechanisms and strategies to examine and address the existing and future cyber threats and one of such efforts has been the drafting of the *National Cyber Security Policy, 2013* in order to provide for the laying down of unified actions against the threats in the

¹ TALAT FATIMA, CYBERCRIMES, 89 (1st ed., 2011) .

² *The National Cyber Security Policy, 2013* (Sept 20, 2018, 3:00 PM), meity.gov.in/content/national-cyber-security-policy-2013-0.

³ Black's Law Dictionary, *what is cyberspace?* (Oct 1, 2018, 11:57 AM), <https://thelawdictionary.org/cyberspace/>

⁴ The Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).



cyber space. The said policy envisions having an integrated approach and a set of sustained and coordinated strategies for implementation.¹

One of such similar efforts of the Government of India has been the recently drafted, the *Personal Data Protection Bill, 2018*.² The Bill starts with the proclamation of the right to privacy as a fundamental right and the necessity to protect personal data as it forms essential part of “informational privacy”.

Reality check

However, the present scenario displays a debatable perspective in practice. In India, the National Crime Records Bureau (NCRB) report of 2016³ highlights the comparative analysis of cyber crimes statistics in India which is, 9622 cyber crimes in 2014, 11592 in 2015 and 12317 in 2016. Uttar Pradesh taking the first rank with 21.4% share of the total percentage of cyber crimes and Assam occupying the first rank as per the crime rate in 2016. The said report shows that the Total Cyber Crimes under the Information Technology Act were 8613, total cyber crimes under Indian Penal Code, 1860 were 3518 and total cyber crimes under Special Local Laws were 186.

The report shows the statistics for Police disposal of cyber crimes State/ UT wise: 12317 cases reported during the year, number of cases withdrawn by the Government - 1, number of true cases but insufficient evidence - 4424, false cases- 276, Mistake of fact - 513. Cases in which Charge sheets were submitted - 3712, cases disposed off by the police - 9213, cases pending investigation - 14973. The report also shows the Court disposal of Cyber Crimes State/ UT wise: total cases for Trial during the year - 10164, no. of Cases Compounded - 40, cases convicted- 201, cases acquitted or discharged - 542, cases dispose off by Courts - 783, cases pending trial - 9381, no. of conviction rate - 27.1%.

¹ *The National Cyber Security Policy, 2013* (Sept 20, 2018, 3:00 PM), meity.gov.in/content/national-cyber-security-policy-2013-0.

² The Personal Data Protection Bill, 2018, “WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy; WHEREAS the growth of the digital economy has meant the use of data as a critical means of communication between persons; WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation; AND WHEREAS it is expedient to make provision: to protect the autonomy of individuals in relation with their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organisational and technical measures in processing personal data, to lay down norms for cross-border transfer of personal data, to ensure the accountability of entities processing personal data, to provide remedies for unauthorised and harmful processing, and to establish a Data Protection Authority for overseeing processing activities; BE IT ENACTED by Parliament in the Sixty-Ninth Year of the Republic of India as follows:”

³ The National Crime Records Bureau (NCRB) report 2016 (Jul 7, 2018, 12:06 PM), www.ncrb.gov.in.



Balancing of interests- important factors

The study of cyber crime has always been traced with conflicting ideas and interests from different parts of the global society. The ever growing discussions have mostly been to debate on the priority or superiority between the concepts of privacy versus surveillance or online freedom of expression versus censorship. In an attempt to understand whether it is possible to strike a balance between these conflicting interests or not, a brief analysis of these factors is essential.

To begin with one such analysis, it is important to briefly study both conflicting ideas. On one hand, what does surveillance mean? Surveillance implies that the authorities are demanding to have an access to the encryption of the technology companies through a “backdoor”. The authorities want to make use of those backdoors as and when required. In simple words, it means that the authorities can take the assistance of any relevant software company to break past the encryption. It is important to note here that the encryption will be strong enough to keep out the cyber criminals. However, what the authorities desire is not 100% of unbreakable encryption but a combination of 99% unbreakable encryption and 1% of backdoor accessibility.¹ On the other hand, what will privacy in these conflicting times mean? With many highly publicized privacy threat cases being highlighted through press/ print and social media, online privacy has become a burning issue. Due to which the privacy of the customers has occupied a top priority attention with the technology companies across the globe. An argument on behalf of those who prioritize online privacy is that the demand by authorities for the backdoor access will not be a welcomed gesture and it will be against the interests of the customers’ privacy. To support the fear of these technology companies, many companies, most notably Apple, have said that creating any kind of backdoor would weaken their overall security since any backdoor has the potential to be exploited by criminals.

When the issue of online privacy is under discussion, it is very important to first learn the modes in which online privacy can be breached or threatened. With the ever growing dependence upon the internet and cyber space, the cyber threat is increasing at an alarming rate as well. Online privacy threats can be traced in the forms of publication of sexually explicit materials, hacking, leakage of confidential information or data, e-commerce frauds, bank frauds, identity theft, cyber stalking, cyber voyeurism, cyber bullying, etc. Today, the threats to online privacy is far more alarming than what it was just few years back. The existence of fear of such threats has impacted nations to enact cyber laws to protect the privacy of their citizens. This fear further leads to the concerns from the Human rights activists as well. It is now known fact that the power, capacity and speed of information technology is accelerating rapidly. The extent

¹ Craig Charles, *The Privacy vs. Surveillance debate. Explained* (Oct 6, 2018, 10:26 PM), <http://techexplained.net/the-privacy-vs-surveillance-debate-explained/>.



of privacy invasion or certainly the potential to invade privacy increases correspondingly. Here, globalization also plays a crucial role in the unrestricted flow of data.

At this point begins the role of the Judiciary. Judicial activism has brought the Right to Privacy within the realm of Fundamental Rights. Article 141 of the Constitution states that “the law declared by the Supreme Court shall be binding on all courts within the territory of India.” The Supreme Court of India has come to the rescue of common citizen, time and again by construing “right to privacy” as a part of the Fundamental Right to “protection of life and personal liberty” under Article 21 of the Constitution, which states “no person shall be deprived of his life or personal liberty except according to procedures established by law”. In the context of personal liberty, the Supreme Court has observed “those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law”.¹

In a broader context, a balance between the conflicting interests between the right to the freedom of expression and privacy can be understood through the following heads:

- i. To what classes of data should the freedom of expression be limited in order to protect privacy?
- ii. In which context will freedom of expression impinge on privacy?
- iii. In what circumstances is it necessary that an individual be provided the right to privacy in order to protect the freedom of speech?

However, there exists certain circumstances in which the freedom of expression may be required to be negotiated. For example, certain circumstances involving public interest, public persons, privacy of minors, responsible role of media and victims of sexual violence are matters requiring sensitive handling.

Another contemporary issue in need of mention is the issue of “online speech”. The impact of social networking sites is much scarier than expected. Today, the right to privacy is equally applicable to online privacy and affects the right to freedom of expression. Today the internet has made privacy an integral part of realizing the right to free expression. For example, governments are putting in place censorship regimes that do not only restrict online speech, but also seek to identify the source of the speech. In this way, the right to anonymous speech has become a contested issue globally. The internet is also making the line between speech expressed in the private sphere vs. speech expressed in the public sphere more difficult to define. It is unclear if statements made on the social media should be considered public or

¹ Meena Ketan Sahu, *Right to Privacy vis-à-vis Cyber Law: National and International Perspective*, 4 **AJMS** (2016) (Nov 1, 2018, 8:14 AM), <<http://www.ajms.co.in/sites/ajms2015/index.php/ajms/article/view/1815>>.



private, and if private individuals posting pictures need consent from all individuals before posting the picture or video on social media sites.¹

In *Shreya Singhal v. Union of India*², the most direct benefit of this judgment is the positive impact that it will have on freedom of speech on the Internet, one aspect of our fundamental rights that has in the recent past been systematically eroded. The Supreme Court by declaring Section 66A unconstitutional acknowledged that freedom of speech applies to the online realm as well. It has also acknowledged that anything said on social media and the internet will provoke or annoy to certain extent but has ruled that even in those cases the government may not curb the rights of individuals to enjoy their fundamental right of freedom of speech and expression. It is only when social media is used to incite persons to public disorder that the restrictions offered under Article 19(2) can be invoked.

On the other hand, it is perhaps unfortunate that the Court did not see fit to apply the same logic to the provisions of Section 69A. However, the decision to read down the provisions of Rule 3(4) and consequently rationalize the benefit of Section 79 of the IT Act to the broad community of intermediaries is likely to have a significant benefit on Indian companies whose business model is based on the Internet.

Concept of responsibility sharing- role of different stakeholders

The important question that arises here is “is legal control the only solution to check the menace of cyber crime?” A brief overview of some of the available literature on cyber crime, it would not be completely wrong to answer the above question in negative. That is, no, legal control is not the only solution to check the menace of cyber crime in the present day scenario where every sphere of the global community is so interwoven and no mechanism to address any socio-legal problem can be successful in solitude. To substantiate the answer, it would be helpful to briefly discuss the roles played by the following stakeholders:

- i. The Legislature: the role of the legislature has never been undermined. It is thanks to the continuing efforts of the legislators that the Information Technology Act, 2000 which is the first ever cyber law in India was enacted. In addition to it, other various Information Technology Rules have been laid down to further strengthen the cyber security in India. However, the present scenario reminds us that law and society are not static but dynamic in nature. As such, the proper way to tackle any problem would be to apply a unified action.
- ii. The Judiciary: the judiciary comprising of the judges and lawyers have a crucial role to play in the administration of justice and bringing the offenders to justice and providing relief to the victims. Through judicial activism, the right to privacy has

¹ Draft, *Freedom of Expression & Privacy* (Oct 4, 2018, 1:39 PM), <https://cis-india.org/internet-governance/blog/freedom-of-expression-and-privacy.pdf>.

² *Shreya Singhal v. Union of India*, AIR 2015 SC 1523 (India).



been declared as a fundamental right under Article 21 of the Constitution of India and it has been equally extended to online privacy in cyber space. With more technologically sound and trained judges and lawyers, the existing and future cyber threats and challenges can be addressed more efficiently.

- iii. The Law Enforcement Officers/ Police: one of the essential pillars of a safe society is the Police. With their trained and skilled methods of investigation and criminal profiling, the computer criminals can be arrested or prevented from committing any cyber crime. Proper training of police officers in dealing with the cases of cyber crime and establishment of more Cyber crime Cells in each Police Station (atleast at Sadar level) would definitely be the secret weapon to tackle the menace.
- iv. The Information and Telecommunication (IT) sectors (both Government and private): with the ever growing need of the services provided by the IT service providers, most of our daily lives have become dependent on them. With the public trusting the service providers with the personal information, the safety of those data is of great concern and as such they are to do their jobs responsibly and without any negligence.
- v. Educators: the educators have always played an important role every time in spreading the knowledge and making complicated concepts simple and understandable to the unknown and ignorant. Children spent atleast eight hours per day in the company and guidance of their educators. As such the influence is great. The educators can spread awareness amongst the students and their parents about the negative effects of allowing the children to use mobile phones at a very young age, open discussions and sharing of pros and cons of internet usage and the social media, child pornography, cyber bullying, hacking, responsible and safe use of facebook, etc.
- vi. Researchers: Cyber space and cyber crime are such area of study in which a continuous research and development is required. Almost every minute, the cyber space is giving birth to more useful as well as dangerous minds. As such, in depth study and analysis of various variables influencing the safety of the cyber space is a must. These research can in turn be used for policy making and sometimes appreciated by the legislators and educators.
- vii. Social Activists/ NGOs: since it is very difficult for the government officials to reach out to every corner of the country, the social activists and the Non-governmental organizations can act as agents for the government and work on behalf of it. These groups of people are known for their vast knowledge of the grass root level masses and as such can be very useful in generating and spreading awareness among the unreachable masses.



- viii. Press/ Print/ Social Media: the press/ print/ social media has now become one of the most quickest and influential medium of generating and dissemination of information. It is a useful tool as well as a dangerous source of data.
- ix. Private- Corporate Partnerships: the collaboration between the private and the corporate sectors can be of great value in terms of data outsourcing and protection of privacy of their customers. The bond of trust is crucial factor here. For example, e-commerce through online transactions, etc.
- x. Parents/ Family: parents and family members play a very important and influential role in the lives of the children. As it is rightly said, charity begins at home. The parents should set examples of good and healthy way of living and be cautious of what they preach and practice.
- xi. Peer Groups: friends make a life- long impact on our lives. Having the right and safe kinds of peer group is important. Especially in the era of internet and social media, having a healthy peer group becomes crucial.
- xii. Private- Public Partnership: since the use of internet has increased by leaps and bounds in the last few decades, it has become almost impossible for the government to keep track of the cyber security of the citizens. In this situation, the private companies are taking up partnerships with the government to work on its behalf and do the needful.

Where we stand? Issues and Challenges

One important aspect of cyber crime is the challenges in acquiring access to justice and appropriate redress to the victims of cyber crimes.

- i. People's apathy and attitude of indifference: one of the biggest challenges in addressing the issue of cyber crime has been the people's lack of enthusiasm or interest in understanding the new problem in depth and taking it seriously at par with any other kind of traditional crimes. Sometimes, the victims are themselves vary of the fact that they have fallen prey to a cyber crime.
- ii. Identity of the offender being unknown: due to the unique nature of the internet and the cyber space, the identity of the offender is most of the times unknown. The offender may commit a cyber crime from any corner of the world and need not require himself to be physically in contact with the victim.
- iii. Apprehension of threat or harassment from the culprit: the fear of being threatened or harassed by the culprit is high in the cases of cyber crime as the identity and the physical location of the culprit is difficult to trace in most cases.
- iv. Social and public indignation: most of the times, the bigger challenge than the crime is the social and public indignation.



- v. Lack of faith and confidence in the police: people are still afraid of approaching the police authorities for reporting a crime. Especially, with the unfamiliar characteristics of cyber crime, the victims are even more confused and afraid of approaching the police. Due to the general notion and common practices of the society, the police authorities have always had to face the lack of faith and confidence from the general public. As such, this creates a vacuum in the proper and prompt action against the culprit and the crime.
- vi. Lack of awareness and education on the issue: since the specie of cyber crime is still new to many parts of the global society, there has been lack of awareness and education on the issue of cyber crime, its nature and impact.
- vii. Lack of infrastructure: whether it may be due lack of funds or lack of interest on part of the government, the lack of infrastructure, lack of enough number of cyber crime cells in each district, lack of cyber forensic laboratories, etc have added to the problem.
- viii. Lack of technological intellect: The lack of planned investments in the building up of technological know- how and skill training of different stake holders at different levels is one big challenge.

Apart from the above challenges, the commission of a cyber crime may lead to victimization of person or persons and it leaves a serious impact on the victim.¹ Such impact may be studied in the form of following heads:

- i. Psychological Impact: One of the most important and grave impacts of cyber crime is the psychological impact. The victimization of a victim in the cyber space leaves an inerrable impact on the victims' mind and psychology, thereby causing various psychological problems and issues hampering their mental health for a certain period of time or in some cases, for a lifetime. For example, in the case of cyber stalking, the particular victim is made to feel discomfort, insecure, scared, threatened, outraged, violated, exploited or harassed, etc. due to the continuous victimization by the offender. These arrays of feelings cause an attack on the psychology of the victimized person. Such fearsome experience cannot actually be put into words. Only the victim has to live with such a trauma.
- ii. Physical Impact: Another aspect of victimization is that it has some physical impact as well. For example, in cases of cyber bullying like "dare games" (the infamous Blue whale) caused such hypnosis of the victims to physically hurt themselves as a series of tasks given by the administrator. Another instance of physical impact would be the luring of the women and children by the online predators and

¹ N. V. PARANJAPE, CRIMINOLOGY AND PENOLOGY (14th edn., 2009).



committing crimes like abduction, rape, physical confinement and torture just for sake of satisfying the offenders mental or emotional and physical void.

- iii. Financial Impact: Last but not the least, another aspect of victimization is the financial impact on the victims. For example, in case of cyber hacking or phishing, the victims end up facing financial loss by the fraudsters.

Conclusion

The fact that the prime approach for tackling any form of crime would be the enactment of a strong legislation for curbing the menace. The practice of undertaking law making process as the first measure to address the problem has been prevalent for quite some time now. However, the fact that we live in the era of globalization and internet cannot be ignored. As such, only the legal control approach may not reap us successful outcomes. The need to strike a balance between the conflicting interests of the citizens has never been felt as intensely as in recent times. For the smooth running of any organization or nation, reaching or establishing a platform or a common ground where sensible discussions can be conducted for greater good of the society at large is pertinent. Thus, instead of using the blocking rule on the modern technologies, it would be ideal if the government devised ways in which both the freedom and privacy could be enjoyed without creating any grounds of chaos and conflict. Keeping intact the value of fundamental rights is equally appreciated in the modern times as well. Another aspect to be highlighted here is the concept of responsibility sharing. Today, mechanism can be successful if it is depended upon only one stakeholder, i.e., the legislators. For the purpose of handling and addressing the unique and new kind of cyber threats, a combined and unified action and effort is the need of the hour. With a reasonable degree of contribution and shared responsibility from different stakeholders in creating a safe society, the existing as well as the future cyber threats can be addressed.

Also further, it is equally important to take note that the nature of cyber crime is unique and different than the other conventional crimes and with the ever growing use of internet, the cyber crime is here to stay and it will be nearly impossible to completely to do away with the problem of cyber crimes. The advanced skills of hackers, birth of new viruses every day, new complications and misuse of the new technology and the indispensable role of internet in the human daily lives make it difficult to completely prevent or control the menace. Hence, it would rather be more meaningful if we work towards regulating and minimizing the cyber crime. Thus, rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activities.



RECOGNIZING PRIVACY AS A FUNDAMENTAL RIGHT - A STEP TOWARDS ROBUST
DATA PROTECTION LAW IN INDIA

Ms. Idyath Barakath Nisha N.,

V B.A.B.L. (Hons),

School of Excellence in Law,

The Tamil Nadu Dr. Ambedkar Law University, Perungudi, Chennai, Tamil Nadu.

Introduction

“Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the state after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State”¹

In the Information Age, we depend information more on our personal data for any activities carried out through cyberspace, this necessitates our own data privacy. As for India concern we not yet have a legal framework for data protection. But this became a burning issue, once the supreme court pronounced right to privacy as fundamental right emanating from Article 21 which is part of our life and liberty, recognized the informational privacy as a part of it.

This gave an attention, a need for legislation and also recommend to draft a robust data protection law to the government. As soon as, the government also made an effort and formed a committee which is headed by Justice BN Srikrishna, the main objective of this committee is the citizen must be the top of the triangle, the rights must be protected at any cost, as well as the trade and industry or entities should not be left out as result of such legislation, should encourage the growth of digital economy globally. Finally, the state has responsibility to protect these rights, to promote trade and business and must empower Indians. With this the committee has come up with a report and draft bill after an extensive consultation with public and stakeholders through report of white paper on this subject. Lastly, it was submitted to the Ministry of law and Justice for further parliamentary process and this makes a discussion on report and bill, how far it makes a way for strong regime for data protection law as supreme court recommended and what extent the bill balance the digital economy and protects the fundamental right to informational privacy.

Evaluating the value of privacy under data protection

To have an idea about data protection one has to understand with the concept of privacy, both are interrelated with one other. But privacy pertains to different context like spatial privacy², decisional privacy and informational privacy. Of these data protection is related with informational privacy but ultimately it impacts on the other two. The sphere of privacy

¹ Justice Chandrachud in Puttaswamy case 2017

² Physical space, bodies and things or physical zone of control over intrusion by others.



includes a right to protect one's own identity. Though privacy is relating with secrecy but it controls over personal information without unnecessary intrusion. Informational privacy provides right to self-sufficiency and determination one's own personal data. There have been attempts made for proposing laws for the protection of data and privacy¹. In 2012, experts panel headed by former chief Justice of Delhi High court AP Shah was set up by the planning commission to identify issues of privacy and to prepare a document (Report of the group of experts on Privacy). It also outlined nine privacy principles² which helps while framing data protection law, but no steps were taken on this recommendation.

Existing Data Protection laws in India

India yet not have any specific Legislation on Data protection, however under Information Technology Act 2000 Section 43A³ compensation for failure to protect data by implement reasonable security and procedures by a body corporate. and section 72A punishment⁴ for improper disclosure of personal information, however it does not provide norms for data collection, storage and processing. In 2011 the government issued IT Rules⁵ (Reasonable Security Practices and procedure and Sensitive personal Data or Information). This rules-imposed requirement relating to collection and disclosure of sensitive personal data which applies only to body corporate and person located in India. Rule 3 provides sensitive personal data, Rule 4 provides to draft privacy policy by body corporate and Rule 5 provides the guidelines need to be followed by entity like obtaining consent, lawful purpose, retain the information required under any law, to maintain security for information provided, designate a grievance officer who shall be responsible to address grievance. Rule 6 imposes prior permission before disclosing to the third party. Rule 8 provides reasonable security practices and procedures.

Aadhaar Act (The Aadhaar Targeted delivery of Financial and other subsidies, benefits and Service) Act 2016, provides protection for Biometric data which obtained Aadhaar number. It mandates the Unique Identification Authority of India should ensure security, confidentiality of identification information and records of individuals⁶

Judicial steps towards legal framework for data protection

Right to privacy case

¹ First attempt made in 2006 personal data protection Bill 2006, presented in parliament, it was consisting of 14 section, but it was not passed. And after the government proposed privacy bill 2011, and Privacy Protection Bill 2013, but not yet any bill passed.

² Principle of notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security, openness and accountability.

³ Information Technology (amendment) Act, 2008.

⁴ Imprisonment for a term not exceeding three years or with fine not exceeding up to five lakhs rupees or with both in case of disclosure of information in case of breach of contract.

⁵ Referred: department of Information Technology issued notification 2011, <http://meity.gov.in/sites/>

⁶ Section 28 and Rule 22 of Aadhaar (Enrolment and update) Regulation 2016 measures for data security.



In 2017, the nine-judge bench of supreme court in puttaswamy case¹ overruled its previous judgements² but Justice Subba Rao in dissenting view opined³ it was a part of personal liberty and upheld the fundamental right to privacy enshrined in the constitution under Article 21 recognized right to privacy as an intrinsic part of the fundamental right to life and personal liberty. It also recognized 'informational privacy' as one of the privacy can be claimed against state and non-state actors

"informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well". We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and a sensitive balance between individual interests and legitimate concerns of the state".

However, the court says it is not absolute right subject to reasonable restriction there may be other interest to consider. To limit the state discretion under the reasonable restriction, court laid down the test that it has to fulfil legitimate aim of state⁴, action must be sanctioned by law, state interference must extent to proportionate to the need for such interference⁵ and there must be procedural guarantee for such interference. Further it directs the government to make a robust data protection regime for protection which against state and non-state actors in the digital age. After that within the year a Justice BN Srikrishna committee has formed to submit a report and draft a bill which was submitted during 2018.

Aadhaar Verdict

After the submission of report, much waited for Aadhaar verdict, finally it comes during September 2018 which held constitutionally valid by 4:1 majority⁶ but struck down certain provision section 33(2)⁷, 47⁸ and 57⁹ for further protection of data which contain under Aadhaar

¹ Justice K.S. Puttaswamy (Retd) v. Union of India & Ors 2017.

² M.P. Sharma v Satish Chandra, (1954) SCR 1077, it observed that search and seizure of documents pursuant to FIR which violate privacy but the supreme court held it is not fundamental right.

³ Kharak singh v State of Uttar Pradesh (1964) 1 SCR 332.

⁴ Justice D.Y. Chandrachud, paragraph 185 says protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits mentions certain legitimate aims of state.

⁵ S.K. Kaul, J., Paragraph 71.

⁶ Justice A.K. Sikri read the judgement on behalf of chief Justice of India Dipak Misra and Justice A M Khanwilkar upheld and dissent opinion by Ashok Bhushan.

⁷ It requires to disclose information for identity and authentication in the interest of national security after approval from anyone equivalent to the rank of Joint secretary.

⁸ This section which allows only the government to complain in case of unauthorised use of Aadhar data, now the individual can also file the complaint.

⁹ It refers the use of Aadhar data by anybody corporate or person to establish the identity of an individual, but it was found to be unconstitutional.



Act 2016. Now after this, it was very clear that verdict Aadhaar Act also serves legitimate state aim by upholding the section 7 of the Act that the government can insist on this Aadhaar identity to grant subsidies and benefits which is the welfare schemes of the government and court also added that those services and benefits should not unduly expanded which will not taken into section 7 and upheld linking of PAN and for filing tax returns¹, however it made unconstitutional mandatory linking of bank accounts² or mobile³ with Aadhaar as it does not satisfy the test which held in puttaswamy case. And it also made CBSE NEET and UGC or any school admission cannot make Aadhaar mandatory.

Formation of Justice BN Srikrishna Committee

In 2017, The Ministry of Electronics and Information Technology constituted committee of experts headed by the former Justice BN Srikrishna to study and make suggestion on data protection law to submit a report along with a draft bill. The main objective is “to ensure growth of digital economy while keeping personal data of citizen secure and protected”. To achieve this a White paper has been drafted which outlines the issues, examines the international practices and what need to be incorporate in a law along with some questions has been framed to receive public responses from public and comments from stakeholders⁴. Nearly after a year of consultation, On July 27 2018 finally the committee submitted its report “A free and Fair Digital economy-protecting privacy, empowering Indians”⁵, to Law Minister Ravi Shankar Prasad, during a press event along with draft, The Personal Data Protection Bill, 2018.

Analysis of the Personal Data Protection Bill, 2018

The Bill recognizes certain provision from Europe Union General Data protection Regulation which recently enacted has come into force in 25 may 2018⁶. However, this draft bill covers the State, Indian Company or citizen or body of person or any other person. It applicable to those who process personal data within India as well those data processors set up outside but process data belonging to Indian Nationals in connection with any business or any activity offering goods and service to data principals within the territory of India⁷.

¹ Section 139AA of the Income Tax Act mandates linking of Aadhaar with PAN upheld in the case of Binoy Viswom v. Union of India.

² The court struck down Rule 9 of the prevention of Money Laundering (Maintenance of Records) Rules, 2005 which instead bank accounts should linked with Aadhaar.

³ Department of telecommunication issued circular on march 2017 mandating linking of mobile number with Aadhaar was held to be unconstitutional was not backed by any law.

⁴ The white paper of the committee of experts on a Data Protection Framework for India consists of more than 240 pages, referred: <http://meity.gov.in/white-paper-data-protection>

⁵ <http://meity.gov.in/>

⁶ Replaces the Data Protection Directives of 1995.

⁷ Section 2 of Draft Bill 2018.



The Bill introduces the concept trust relationship between data principal and data fiduciary. The Bill also makes the person who processing the personal data as a Data fiduciary and who process on behalf of a data fiduciary is a data processor and Data principal is the natural person whose personal data is referred, whereas under EU GDPR it considered as data subjects and data controller. section 5 of Bill introduces purpose limitation, it shall be processed only for purpose specified it must be clear, specific and lawful. The data fiduciary shall notice data principal at the time of collection of personal data which include purpose, categories, identity and contact details of data fiduciary, data protection officer etc¹. the bill provides privacy by design which mandates data fiduciary to implement policies and measures to protect personal data from the point of collection to deletion of data and uses of technology must be certified standards². Section 36 of bill mandates to appoint data protection officer who provides advices on matters relating to fulfilling obligation under this Act, maintaining all records maintained by the data Fiduciary. The Data protection authority³ duty to protect the interest of data principal who monitoring and enforcing provision the bill. Power to issue direction, call for information, to conduct inquiry and also action can be taken by the authority pursuant to enquiry, including search and seizure and for imposing penalties or awarding compensation there will be adjudicating officer who have ability, integrity and must have special knowledge and experience in field of law relate to this.

Critical analysis on issues and challenges of the Bill 2018

No Data Ownership

The Bill introduced the concept trust relationship of data principal and data fiduciary other than data ownership. Justice BN Srikrishna explained the concept of trust relationship during the press conference why there was no data ownership. He answered, the ownership of data is something to do with property but matter of trust is entrusted with somebody he is answerable and it must be used fairly so data principal expects various level of trust and loyalty and data fiduciary duty to care fairly and fulfil the expectations reasonably expected by the principal, although the GDPR and other countries used data Subjects.

Exception for processing personal and sensitive data without consent

The fundamental principle under data protection law is lawful processing. The European Union GDPR says that it should be transparent, it should be consulted or otherwise processed to what extent the personal data will be processed⁴. OECD guidelines also recognizes the collection of

¹ Refer section 8 of Daft Bill.

² Section 29 of Draft Bill

³ Chapter X of draft bill 2018 deals with Data protection Authority of India.

⁴ Article 5 and Recital 39 of EU GDPR.



personal data must be lawful, fair means and with the consent of individual¹. The bill 2018 also allows that processing of personal data must be done only for clear, specific, and lawful on the basis of consent is obtained². In case of processing sensitive personal data, it should be based on the explicit consent. But the provisions also allow the government can process the data without the consent if it necessitates for any function of parliament or state legislature or providing benefits, services, issuing of licenses, or required under the law. Under this, Government seems to have overarching power when it comes to processing the data and this exception may dilute the rights of person with respect to data privacy. The thinking behind the committee is, under some situation relying solely on consent would be difficult for all day to day processing activities would lead to multiple of notice for consent. However certain lawful grounds need to designate to allow flexibility of such activities and to achieve the purpose of activities even in the absent of consent. To justify, committee taken up the view of EU GDPR which provides that data processing based on subject consent or other basic five grounds³.

Right to be Forgotten

It is common for internet users to reveal information, later they wish to remain secret. The Indian judiciary also recognised the right to be forgotten in high sensitive cases like rape or reputation of person. The importance of this right emphasised by the supreme court in puttaswamy case, it observed that right to privacy which derives right to remove the shackles of unadvisable past things. EU GDPR emphasize the right to be forgotten, the service provider shall have the obligation to erase when the demands of erasure of personal data without undue delay unless the retention of data is necessary for exercising right of freedom of speech and expression⁴, but the decision regarding right to erasure is left on the data controller.

The draft bill provides four rights to data principal, right to confirmation and access, right to correction, right to data portability and right to be forgotten which similar rights under GDPR. However, the right to be forgotten⁵ will be able to restrict or prevent continuing display of personal data once the purpose has ended or consent has withdrawn by data principal. But the bill does not allow for complete erasure as the GDPR has strict right. A data can be retained for reasonable not necessarily to erase it. But this is not what right to be forgotten is referred

¹ OECD Guidelines on the protection of privacy and transborder Flows of Personal Data (2013), Referred: <http://www.oecd.org/sti/economy/oecdguidelines>

² Where the data principal withdraws consent, all legal consequences for such withdrawal shall be borne by the data principal, refer: section 12(5) of bill.

³ Refer: Article 7(a)-(f), EU GDPR says Performance of contract, legal obligation, vital interest, public interest task, or exercise of official authority, legitimate interest subject to additional balancing test against the data subject rights and interest.

⁴ Article 17 EU GDPR and Article 85 says the exception to remove data for journalistic, academic, artistic or literary expression purposes.

⁵ Section 27 of Draft Bill 2018.



around the world. But Justice Srikrishna during the press conference he answered that, for historical research or statistical concern or obligation under any law to assess or defence of legal claims it requires to be part of record in some cases.

Data localisation and condition on transborder transfer

It requires the entities to store and process data on servers physically within national borders and transfers outside the country subject to safeguards. Even the RBI mandates all data generated by the payment system in India must be stored within India. The draft bill 2018 makes restriction and condition¹ for the cross-border transfer of critical or sensitive personal data by entities. It makes its data fiduciary mandatory to store at least one copy of all person data of India Nationals must be stored on serves or data centre located in India. The central government have discretion to notify certain categories of personal data which is a critical data that must be processed only in India² for the national interest. Thus, the committee intended that free flow of data is norm and to restrict as an exception, in other words the destination is across borders, but it would need to be stored local in India. Experts believe that this requirement in the Bill does not help in protecting the privacy of individual may leads to state surveillance. Even the dissent view³ from members of committee Rama Vedashree⁴ who says that this requirement is regressive against the fundamental tenets of the liberal economy and she also added that localisation could be a trade barrier. The other member prof. Rishikesh⁵ has dissent view that every data fiduciary should store one live, serving copy of personal data in India is against the basic philosophy of the internet.

But the white paper report suggested that it protects the rights of data subjects and its enforcement agencies will have access to more data against crimes and prevent foreign surveillance and it also referred some of the countries⁶ have the practises of data localisation but the GDPR does not impose such but it requires to transfer data only the country which have safeguards for data protection.

¹ Section 41 says subject to standard contractual clause or intergroup schemes approved by authority or any international organisation or particular set of transfer is permissible or data principal consented to such transfer explicitly.

² Section 40 and 41 of Draft Bill 2018.

³ Referred: report of "A free and Fair Digital economy protecting Privacy, empowering Indians" Note on the Personal Data protection Bill 2018

⁴ CEO of NASSCOM Data Security Council of India

⁵ IIM Indore professor.

⁶ Russia enacted Federal Law Article 16(4)(7) No.242-FZ which mandates data operators must store with data centres located in the territory of Russia and must also notify Russian Data protection authority the location of servers where the data is located. In china, Article 37 of Chinese Cybersecurity Law 2016 states operators in china must store data domestically on Chinese servers.



Data breach notification

It refers to alerting about personal data has been breached which can be unauthorised disclosure or access to, alteration, unlawful destruction may result in physical, material or non-material damage. Any data breach is likely to cause harm to data principal, the data fiduciaries should first inform to Data Protection Authority of India (DPAI) who determine whether it need to inform the data principals about the data breach even if it is highly cause. Breach notification includes subject matter, number of data principals affected, possible consequences and measures being taken to remedy the breach¹. But there is some criticism about informing to DPA first but not to the real owner of data or data principal even DPA will determine whether it need to be inform or not, which is unreasonable and lacks in transparency and accountability. But the head of the committee shrikrishna recommended that rectification measures or assessment of consequential damages is better to left with the regulators², otherwise it cause multiple notification each and every day to the data principals.

Penalties³ and Criminal Liability

Section 69 of bill makes data fiduciary liable for the penalty for any contravenes of provision would be Rs 15 crores or 4% of the total worldwide turnover of preceding financial year and failure to take prompt action on a data breach would be Rs.5 crores or 2% of turnover whichever is higher as a penalty. Certain data breach which are extremely serious, it may be authoritative to prescribe criminal sanction in the form of punishment and heavy fines. Section 90 of bill says any person in contravention of provision of the bill shall be punishable with imprisonment not exceeding three years or shall liable to fine which may extend up to two lakhs or both. In case of sensitive personal data shall be five years not exceeding or liable to fine up to three lakhs which is also cognizable and non-bailable offence⁴

Need to amend other statutes⁵

The committee has identified more than 50 Statutes overlap data protection framework with this bill, it will override the sector like RBI, SEBI and recommended the concerned ministries to take of this and ensure measures for harmonizing amendments which is necessary. Even committee mentioned the Aadhaar Act need to be amended to bolster data protection which includes offline verification of Aadhar number and to ensure autonomy of UDAI and committee

¹ Section 32 of draft bill 2018.

² Even EU GDPR requires in case of breach the controller shall notify the breach within 72 hours under the Article 33(1).

³ The IT Act does not prescribe civil penalty provision for any failure of data obligation

⁴ The member of committee Rama Vedashree has dissent view that inclusion of criminal offences along with fines is excessive.

⁵ Referred: Report of the bill chapter 7 allied laws impacted by draft data protection Laws in India, Annexure C.



also recommends to amend section 8(i)(j) RTI Act to have balancing act between public interest and to protect data principal.

Conclusion

The draft bill affords more rights to data principal over their data and makes a greater control over their personal data by preventing others from intrusion through elaborate grievance mechanism for such breach of privacy. Although the principle of consent has been highly diluted by creating many exceptions for processing such data by government. Even though the bill is uncertain about certain matters and far being perfect, this is not going to be final law which requires the application of mind, consultation and parliamentary process. As the Law minister has rightly pointed out during press conference that there will be consultation, scrutiny, cabinet approval as such would go through multiple stages before reaching the parliament. However, the formation of committee, comprehensive report and draft bill may be as a first step to form a regime for data protection law, it might be necessary to fine tune the law as technology keep changing.

Suggestion

In several areas of draft bill, it necessary to have wide parliamentary and inter-ministerial discussion before it comes into the law.



**JURISDICTION AND TERRITORIALITY OF THE CYBERSPACE, IN THE ASPECT OF
MUNICIPAL AND INTERNATIONAL LAW**

Ms. OVIYA Nila Muralidharan,

*IV B.A.LL.B. (Hons), School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law
University, Perungudi, Chennai, Tamil Nadu.*

INTRODUCTION

“It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person”¹

With the apt words of the first Section of the Information Technology Act of 2000, there can be none better to explain the complexity and technicality associated with the jurisdiction and territoriality of any law governing the cyber space. To begin with, it is imperative to understand that with any law, comes the three main aspects of it, the sovereignty of the state that passes it, the territory and extent of such state and finally, the jurisdiction that is extended. In such a regard, it is often found to be difficult to associate these aspects to any issue, when it is one that ranges beyond the territory of just one state.

This paper shall look into the jurisdictional aspects of issues crossing border, the situation of cyber law in such a cross-road and finally, the Indian application to the system of cyber law around the world.

JURISDICTION IN INTERNATIONAL LAW

Jurisdiction in its plainest sense is ‘the authority of a court or official organization to make decisions and judgments’² The authority of such court is derived from, as seen above the various factors that influence the applicability of the law. In the context of jurisdiction, the application can be seen from two lenses, namely³;

- **Prescriptive Jurisdiction**

This type of Jurisdiction involves the state’s ability to make laws in respect of any avenue or field it chooses to be applicable irrespective of the person committing it.

- **Enforcement Jurisdiction**

Unlike the former type, this jurisdiction is largely dependant on the enforcement of the laws so made as seen above. Herein, there arises several issues about the concomitance of states, the respect for another state’s

¹The Information Technology Act (2000), Section 1(2)

² Concise Law Dictionary, Sumeet Malik, Eastern Book Company, 2015

³ Personal Jurisdiction in Cyberspace,

Available at: http://shodhganga.inflibnet.ac.in/bitstream/10603/7829/14/14_chapter%205.pdf



sovereignty, and so forth. It thus becomes evident, that on basis of enforcement, the jurisdiction of a state is limited, and it is in this regard, that it becomes even more important to understand the position of cyber law in the space.

TERRITORY IN CYBER SPACE.

While looking into the nature and mode of function of the cyber space, it becomes obvious that the working of the cyber structure transcends the physical boundaries put forth for the application of law. As stated by David R Johnson and David Post¹, "The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules."

In such a scenario, wherein it is an established fact that there lies much confusion and grey area in the application of any municipal law, for that matter to the cyber space, there arises the question as to how, on both a national and international scale, the cyber space can be regulated. Although there is quite a bit of literature developed in this regard on an international scale, the method followed up till now and even now, would be tightening the leash of the national law, protecting boundaries, even on the cyber space, largely by monitoring and regulating the flow of information from within a territorial space to anywhere outside.

However, herein, it has been the regard of several scholars that such a system would sooner or later prove to be futile. As regarded by Professor Peter Martin, who emphasized that such system would be impossible for any nation desiring to participate in global commerce. He stated that, "Physical roads and ports linking sovereign territories are few in number, and geographical boundaries can be fenced and policed. In contrast, the number of starting points for an electronic "trip" out of a given country is staggering, consisting of every telephone capable of connecting outside the territory. Even if electronic communications are concentrated into high volume connections, a customs house on an electronic border would cause a massive traffic jam, threatening the very electronic commerce such facilities were constructed to encourage."². In his words, the 'infinite boundary' of the cyber space makes it difficult, and if attempted, an open ground for much lacunae if simply the states controlled what they regarded as within their borders.

TERRITORIALITY PRINCIPLE OF JURISDICTION

As seen above, it is quite incomprehensible to arrive at the most suitable jurisdictionary applicability for issues of the cyber space. However, in so doing, in the past, it is of opinion that

¹David R. Johnson; David Post, Law and Borders--The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367 (1996)

²Professor Peter Martin, Comment at the NewJuris Electronic Conference (Sept. 22, 1993)



the following two types of jurisdiction¹ must have held an upper ground. The two aspects are largely based on the territoriality principle of jurisdiction and thus, while keeping the essence of the physical border intact, has emerged and adapted to the growing cyber law.

- **Subjective Jurisdiction**

This type entails that the state may make any laws to punish for any crime that is physically committed within one state, that is, the perpetrator of the crime has done such crime within the territory of that state.

- **Objective Jurisdiction**

This type entails that the state may make any laws to punish for any crime that maybe committed or commenced at any part of the world, but has thus caused the occurrence of the crime within the territory of the state. In the plain sense, the perpetration of the crime should have the object to make a certain crime occur in a certain place.

While looking at the above two aspects of the territorial principle of jurisdiction, one can understand that the play of sovereignty of a state is of utmost importance. In the *SS Lotus Case*² it was regarded by the Permanent Court of International Justice that “the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.”

JURISDICTION OF THE CYBER SPACE ON AN INTERNATIONAL SCALE

In viewing the difficulties as seen above on the application of jurisdiction by any one state on the cyber space, the United Nations Commission of International Trade Law (UNCITRAL) came up with the Model Law on Electronic Commerce (MLEC)³ in 1996 as a mode to facilitate and regulate electronic commerce, while providing ‘national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce’⁴

The MLEC not only aimed at a non-discriminating all nation law for the cyber space, but also one that was concomitant and uniform throughout the world. In stating its objectives, the MLEC notes that only with such an implementation, could the overall growth and development

¹Two Aspects of the Territorial Principle, Available at:

http://www.kentlaw.edu/faculty/rwarner/classes/carter/tutorials/jurisdiction/Crim_Juris_16_Text.htm

²*S Lotus Case (France v. Turkey)*, PCIJ Ser A (1927), No. 9

³Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, UNITED NATIONS PUBLICATION Sales No. E.99.V.4 ISBN 92-1-133607-4

⁴UNCITRAL Model Law on Electronic Commerce (1996), Available at:

http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html



of the cyberspace and so forth, technology be achieved. In one of its primary objectives, it was states, “ the establishment of a model law facilitating the use of electronic commerce that is acceptable to States with different legal, social and economic systems, could contribute significantly to the development of harmonious international economic relations,”, which further brings forth the point that smooth international relations can be better achieved by the uniform application of laws by the nations to govern the cyberspace.

JURISDICTION OF THE CYBER SPACE IN INDIA.

The Indian response to the jurisdiction and territoriality of the cyber space was one that was derived from UNCITRAL’s MLEC> The Information Technology Act of 2000 passed by the Indian Parliament was a direct response to it as well. In the Introduction of this paper, a few words that formed the Applicability of the Act was put forth. It highlighted, in a contrast from most other enacted statutes in the country, the application of whose was not limited by simply the territory of India, but well beyond the physical boundaries as well.

It is provided in the Act,

“The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.”¹

in a manner that simply puts forth the preposition held by the applicability under Section 1 of the Act. However, it is also further provided that,

“Further this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.”²

Herein, one can see the application of the Objective aspect of the Territoriality principle of Jurisdiction as seen above inculcated within the essence of this provision. It provides that any person committing a crime from anywhere in the world, would be brought under the jurisdiction of this Act, and thus automatically, the Indian Courts if the crime involved any computer, computer system or computer network located within the physical boundary of India.

In this regard, it can be seen that the Indian law has also applied and further contributed to bringing about a uniform system of jurisdictionary application and law for the cyber space, along with the members of the UNCITRAL

JURISDICTION OF THE CYBER SPACE IN THE OTHER STATES OF THE WORLD.

The current status of the MLEC shall provide much light on the question of jurisdiction in the cyber space around the world. Of the 150 signatories of the UNCITRAL, it is currently seen that only 71 countries have implemented it within their municipal law. While most of them come under the banner of developing nation, the United States of America, also being a

¹The Information Technology Act, 2000; Section 75 (1)

²Ibid; Section 75 (2)



signatory can be viewed in its judicial precedent to better understand the application of such provision.

In an incident in the November of 2014, a previously unknown group calling itself the "Guardians of Peace" breached protected computer networks of Sony Pictures Entertainment, stealing data and disabling computer systems¹. Computer security experts and investigators suggested that the Democratic People's Republic of Korea ("DPRK" or "North Korea") was behind the breach because of certain features in the code used in the attack and Sony's impending release of *The Interview*, a film about killing Kim Jong Un, the leader of the DPRK². Shortly after U.S. President Barack Obama publicly blamed North Korea for the breach and pledged a proportional response, North Korea's internet suffered widespread, catastrophic outages without explanation. One can only assume these outages were due to an American cyber operation.³⁴

CONCLUSION

While several aspects of jurisdiction and territoriality were seen above, and its due application in both the international and national sphere, it is evident that regulation of the cyber space and thus the related principles have much to grow around the world, and has much more unrecognised grey areas. For example, the Sony incident in the United States brought out the entire avenue of *jus ad bellum*, that is, the law of the war aspect in the cyber space. With such gaping holes, it is the emergent need for much more research and development in this field so as to ensure the just regulation of the cyber space, while protecting and preserving the sovereign nature of the nations.

¹Nicole Perlroth, *Sony Pictures Computers Down for a Second Day After Network Breach*, N.Y. TIMES (Nov. 25, 2014), <http://nyti.ms/1rqG41n>.

²Jim Finkle, *North Korea Surfaces in Sony Investigators' Probe into Hack*, REUTERS (Dec. 4, 2014), <http://www.reuters.com/article/us-sony-cybersecurity-investigationnkor-idUSKCNOJH28920141204>.

³See *North Korean Websites Back Online After Shutdown*, TIMES-PICAYUNE (Dec. 22, 2014), <http://www.nola.com/science/index.ssf/2014/12/north-korean-websites-back-oni.html>; David E. Sanger, Michael S. Schmidt & Nicole Perlroth, *Obama Vows a Response to Cyberattack on Sony*, N.Y. TIMES (Dec. 19, 2014), <http://nyti.ms/lv0KOi9>.

⁴Thomas Payne, *Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations*, 20 Lewis & Clark L. Rev. 683 (2016)



CYBER ATTACKS FROM CRIME TO WAR – PERSPECTIVES IN INTERNATIONAL LAW

Mr. M. Sivaraman,

Ph. D. Scholar, School of Excellence in Law,

The Tamil Nadu Dr. Ambedkar Law University, Perungudi, Chennai, Tamil Nadu

&

Ms. S. Jeevitha,

II B.A.LL.B. (Hons), VIT School of Law, Chennai, Tamil Nadu.

Introduction:

Cyber attacks are enacted in myriad forms and for a variety of reasons by state and non-state actors which can also transcend from crimes and terrorism to war dimensions. These attacks could take various forms like denial of service, distributed denial of service, ransomware, viruses, worms, spyware/adware, trojans, attack vectors, social engineering like phishing and pharming, SQL injection, drive-by, man-in-the-middle which can cause various effects ranging from disablement of the network, espionage, data theft, denial of services, malfunctioning etc. These attacks could be targeted against any networked systems in any sector, governmental, military or private, from anywhere in the world giving almost absolute anonymity and impunity to the perpetrators which in some cases also enable them to cover-up their trails, and worse in several cases the detection of such cyberattacks itself is not noticeable early in the stages by its victims. The responsibility of the States in the international legal regime for permitting their soil to be used for exporting cyber terrorism is now getting increasingly sharper focus, definition and delineation. The liability of the victim States to protect its citizens and critical infrastructure from cyberterrorism related disasters, injuries or economic damages is also now being globally and nationally underscored by the judicial pronouncements, international conventions and domestic legislative and policy prescriptions.

Instances of Cyberwar:

Critical infrastructure like the airports, seaports, roads, railways, telecommunication, power generation and distribution networks, health and emergency services, banking system, water distribution and the like for the distribution of essential infrastructure services are these days increasingly catered to by private actors globally, with the governmental participation in such services getting increasingly marginalised. In such scenario, any cyberattacks mounted over computer networks supporting such private critical infrastructure by alien enemies or states or even by non-state actors can have crippling and debilitating effect for nations. The United States acknowledges that the complex network of interdependence of such critical



infrastructure creates a new dimension of vulnerability posing unprecedented national risk¹. Terrorist attacks over information technology and its dependent infrastructure may threaten international peace and security if left unaddressed². In several cases, organisations both in the public and private sector do not publicly admit that their systems have been compromised by cyberattacks and mostly try to shield them from public attention and resort to only restoration efforts privately.

India ranks third in the world to being exposed to cyberattacks³ and over the last 12-18 months period, Indian companies have suffered financial damages to the tune of USD 500,000 due to cyberattacks⁴. Malware cyber-attacks on State Bank of India recently forced it to re-issue around 6 lakhs debit cards⁵, while Union Bank of India had almost lost USD 170 millions when malware codes to transfer funds came to be detected and the fund transfer blocked⁶ in the nick of the time. Jawaharlal Nehru Port Trust's operations had to be temporarily shut down in June 2017 for the second time after the WannaCry attack⁷ and it is also apprehended that cyberattacks on Indian railways can lead to derailment of trains causing accidents⁸.

Elsewhere globally, there have been much more damaging instances of cyberwar attacks, such as the Stuxnet worm attack which had crippled the Iranian nuclear power reactors for several years before it was eventually detected which is attributed to be the handiwork of the intelligence agencies operated by the United States and Israel⁹, while the mass cyberattacks on the erstwhile members of the Russian federation viz. Georgia, Estonia and later Kyrgyzstan are linked to the hackers set up by Russia¹⁰ and the same country is also accused of launching cyberattacks on the electricity grid systems which blew out power supply in Kiev and other

¹US President's Commission on Critical Infrastructure Protection, 1997 Report on 'Critical Foundations: Protecting America's Infrastructure'

²A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, July, 2015.

³ <https://economictimes.indiatimes.com/tech/internet/india-ranks-3rd-among-nations-facing-most-cyber-threats-symantec/articleshow/63616106.cms> as last visited on 30.10.2018

⁴ <https://economictimes.indiatimes.com/tech/internet/indian-companies-lost-500000-to-cyber-attacks-in-1-5-years-cisco/articleshow/63019927.cms> as last visited on 30.10.2018

⁵ See The Indian Express, October 21, 2016.

⁶<https://www.firstpost.com/tech/news-analysis/recent-cyber-attack-on-union-bank-in-india-was-similar-to-the-hack-attack-in-bangladesh-cyber-heist-3700825.html> as last visited on 16.10.2018

⁷<https://www.india-briefing.com/news/massive-data-breaches-cyber-threats-india-15405.html/> as last accessed on 16.10.2018

⁸ <https://www.businessinsider.in/Railway-systems-could-be-hackers-next-big-target-and-derailing-trains-wouldnt-be-that-hard/articleshow/64217842.cms> as last visited on 16.10.2018

⁹ <https://www.csoononline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html> as last visited on 30.10.2018

¹⁰ Andrzej Kozłowski, *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, European Scientific Journal, February 2014, Special Edition Vol.III, pp-237-245



cities in Ukraine¹. Russia is also accused of hacking and divulging the email exchanges of the Democratic candidate Hilary Clinton in the United States' 2016 presidential election and building a negative public opinion against her so as to swing the votes in support of Trump², while the WannaCry ransomware decapitated the national health services of several countries including United Kingdom³. The NotPetya cyberwar ravaged several computer networks in various countries and created a grinding halt to critical operations of ports, shipping lines, logistics, food and several industries including hospitals across the globe and billions of dollars was lost⁴.

Are Cyberattacks an Act of War?

In the case of a conventional war, there are factors such as use of force, armed attack, military object and combatants and state responsibilities which are vividly discernible. But, in the case of cyberwars, these aspects may be greatly masked and be enacted by a few players well beyond the borders of a country by using sophisticated cybertools and malware. It is debatable whether such attacks can be equated to 'armed attacks' and be falling within the scope of 'Law of Armed Conflict'. In the case of *jus ad bellum*, there are well recognized principles like distinctivity, military necessity, proportionality and humanity for initiating an armed response to an armed attack. All or most of these factors may be lacking in the case of cyber wars since it cannot be distinguished as to who is a cyber combatant and a civilian. Or, will there be a military necessity to respond if only civilian infrastructure is affected by a cyberattack or if there is only a defacement of governmental websites or denial of service attacks, will it call for a military response and if so what should be done with the principle of proportionality and against whom such attacks be directed, as most perpetrators are only non-state actors and should the armed response to an attack be conducted in a fashion without affecting the lives of the civilians of the targeted country are some of the issues which do not have global consensus. These uncertainties continue to plague the international law protagonists till date. Despite there being overwhelming accusations against some countries of having unleashed cyberwars on them, yet, till date none of the victim nations have launched an armed response against such perpetrating

¹ See <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/> as accessed on 19.10.2018

² See <https://www.theguardian.com/commentisfree/2018/oct/22/russia-cyber-theft-trump-us-election-president-clinton> as last accessed on 30.10.2018

³ See <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware> as last accessed on 17.10.2018

⁴ See <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> as last accessed on 17.10.2018



nations¹ and on the contrary such attacks were met with a limited use of law and policy to combat them with the response posture defined by restraint².

Article 2(4) of the UN Charter prohibits states from employing “*the threat or use of force against the territorial integrity or political independence of [another] state, or in any other manner inconsistent with the purposes of the United Nations*” and the prohibitions of Article 2(4) are recognized as customary international law, binding not only the parties to the UN Charter but also on all states across the globe. Thus, states may not threaten to use or actually use force against another state, unless an exception is carved out within the UN Charter. Article 2(3) of the UN Charter further enjoins the states to “*settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered*”. The use of force by a state is permitted only when actions are authorized by the UN Security Council or when acting in self-defence. Although Article 42 of the UN Charter enables the UN Security Council to pass a resolution to use military force to restore international peace and security, which it can do so only when it determines under Article 39 that a “*threat to the peace, breach of the peace, or act of aggression*” exists. Once the Security Council determines that this threshold has been met, it can attempt to restore international peace and security in accordance with Articles 41 and 42 of the UN Charter. Article 51 of the UN Charter proclaims that “[n]othing in the present Charter shall impair the inherent right of [states to engage in] individual or collective self-defense” in response to an “armed attack” and this also exists as an inherent right under customary international law. In *Corfu Channel* case³, the International Court of Justice held that states have a duty “*not to allow knowingly its territory to be used for acts contrary to the rights of other states.*” The question whether the Law of Armed Conflicts (“LOAC”) applies to cyberspace was indirectly answered by the International Court of Justice (ICJ), in its 1996 *Nuclear Weapons* Advisory Opinion, holding that LOAC applies to “*any use of force, regardless of the weapons employed.*” The United States in its 2011 *International Strategy for Operating in Cyberspace* holds that “*the development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior – in times of peace and conflict – also apply in cyberspace.*” Article 36 of 1977 Additional Protocol I, requiring testing of new weapons and weapons systems for conformance with LOAC, illustrates that the law of war and international humanitarian law (IHL) rules apply to new technologies. The Tallinn Manual is an attempt to apply the existing body of international law to the

¹Carl Fitz, *All is Fair in Love and Cyberwar: International Law and Cyber-Attacks*, Houston Journal of International Law, 2017, Vol.1, pp.1-17.

²Pauline C. Reich et al, *Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity*, European Journal of Law and Technology, Vol.1, Issue 2, 2010.

³ *Corfu Channel* case (Merits), 1949 I.C.J. 4, 22 (Apr.9)



irregularity of dangers emanating from cyberspace¹. The Council of Europe's Convention on Cybercrime addresses a wide range of crimes against information networks and computer related offences. The UN Global Counter-Terrorism Strategy's CTITF Working Group on Protection of Critical Infrastructure including internet is another important framework². The Tallinn Manual 2.0 (which is a NATO-sponsored effort lacking wider representation of other nations) emphatically declares that international law applies to cyber warfare³. There are also international prescriptions⁴ that states are responsible for private actors who are operating under their direction and control which principle can be extended to cyberattacks launched by them on victim states. The virtual control test can hold a sovereign state to be responsible for the attacks carried out by its internet operators unless it is able to rebut the presumption of responsibility by cooperating with the victim state's attribution efforts⁵. The fact that a cyber-attack is unlawful does not necessarily mean that armed force can be used in response, but, states may be entitled to resort to countermeasures such as "active defences" so long as they comply with the relevant procedural requirements and the principles of necessity and proportionality⁶ and some also feel that mitigative counter-strikes can be sustained within the existing framework itself⁷. In cases like alleged interference in the US President 2016 electoral process by Russia and for related malicious cyberattacks said to be carried out by it, only sanctions were imposed by the United States against it⁸. European Union has promulgated a directive to improve cooperation on cyber security which now requires them to meet a minimum threshold of cyber defences. Canada, United Kingdom, Russia and Australia have also put in place robust strategies to ward off cyberattacks.

Uncertainties Arising out of Cyberwar:

The technological and legal response to cyberwar attacks can be highly ineffective and almost remain invincible as had happened in the case of the leak of the US diplomatic cables by the

¹Oliver Kessler and Wouter Werner, *Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare*, Leiden Journal of International Law, 2013, 26, pp.793-810

²UN General Assembly A/RES/60/288 dated 8 September 2006.

³Rule 80 of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare 375 (2d ed. 2017)

⁴International Law Commission, Responsibility of States for Internationally Wrongful Acts, GA Res 56/83 annex, UN Doc.A/RES/56/83, December 12, 2001.

⁵Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, Melbourne Journal of International Law, 2013, Vol.14, pp.1-24.

⁶Oona A. Hathaway *et al*, *The Law of Cyber-Attack*, California Law Review, 2012.

⁷Jay P. Kesan & Carlos M. Hayes, *Mitigative Counter-strikes: Self Defense and Deterrence in Cyberspace*, Harvard Journal of Law and Technology, Vol.25, No.2, Spring 2012, pp.429-543

⁸See <https://www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html> as last visited on 19.10.2018



Wikileaks¹ and as witnessed in the case of leak of the US intelligence activities by Edward Snowden, which is regarded as an act of 'public service' by acting as a whistle-blower². It is also felt that even the Tallinn Manual does not address the problematic area of cyber espionage³.

At the same time, a review of the existing global literature on the subject reveals views echoing extreme positions. Shen Li argues that to confront the issue of Distributed Denial of Services attack, the principles of self-defense under the international laws should be interpreted through the 21st century lens to authorise self-defense against such cyberattacks within the existing system⁴. The World Economic Forum⁵ has highlighted that the challenges that face cybersecurity are (i) international fragmentation; (ii) lack of consensus in international norm setting; (iii) role of the private sector; (iv) misalignment of incentives for cybersecurity best practices; and (v) ecosystem complexities.

It is opined that until the international comity of states decide to change the law by some other body of law or norms, the effects of cyber warfare will remain ambivalent⁶. The existing system suffers from uncertainty, complexity and insufficiency⁷ and it is exhorted by Tarah Wheeler that globally we desperately now need a digital Geneva Convention, as the present regime of 'armed attacks' do not answer adequately these cyberattacks⁸. It is also opined that this global threat may only be effectively met by a global solution of internationally designing a new law for cyber-attacks⁹ and in line with this notion Boylan also concludes that the ideal solution would

¹ The efforts of the US administration to take down the server of Wikileaks failed with several thousand mirror hosts set-up. So also the legal efforts to apprehend and prosecute Julian Assange of Wikileaks continues to till date remain unsuccessful for more than 8 years, after he has secured asylum in the London embassy of Ecuador country.

² Andrew Buncombe, Edward Snowden: Former Top US Law Official Says NSA 'Whistleblower' Performed 'Public Service', Independent, May 30, 2016

³ Yoo, Christopher S., *Cyber Espionage or Cyberwar?: International law, Domestic Law, and Self-Protective Measures*, (2015). Faculty Scholarship. Paper 1540, University of Pennsylvania Law School.

⁴ Sheng Li, *When Does Internet Denial Trigger the Right of Armed Self-Defense?* Yale Journal of International Law, 2013, Vol.38, pp.179-216

⁵ World Economic Forum's White Paper – Global Agenda Council on Cybersecurity.

⁶ Gary D. Brown, *International Law Applies to Cyber Warfare! Now What?* South Western Law Review, 2017, Vol.46, pp.355-377

⁷ Duncan Hollis, *New Tools, New Rules: International Law and Information Operations*, G.J. David and T.R. McKeldin (eds.), *Ideas as Weapons: Influence and Perception in Modern Warfare* 60 (2004).

⁸ See <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/> as last visited on 17.10.2018. See also, Murat Dogulet al, *Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism*, 2011, 3rd International Conference on Cyber Conflict.

⁹ Oona A. Hathaway et al, *The Law of Cyber-Attack*, California Law Review, 2012.



be an international agreement on the subject¹. It is also suggested that even weak measures such as Code of Conduct or a Confidence Building Measure approach could be adopted to act as voluntary pledges by state parties in the matter of preventing cyber warfare². Kubo acknowledges that in relation to the cyber warfare, a systemic shift has taken place moving from regulatory focus from the law of war to general international law and there is a new trend towards functionality test for state sovereignty and unique teleological underpinning of the law of war is to be taken into account rather than a blanket transplantation of existing body of LOAC³. Kilovaty concludes that the severity of a cyberattack on critical infrastructure being highly devastating, excluding such attacks from the scope of use of force and leaving it in a legal vacuum is not in conformity with the goals and spirit of the UN Charter and the international community values⁴. Fitz advocates that the UN agency of International Telecommunications Union which governs information communication technologies could be strengthened and tasked to address cyberattacks and in order to clarify the applicability of attribution to cyber-attacks, he exhorts that an international agreement and a global forum that initiates a dialogue about these standards is essential⁵. It is also advocated that the definition of aggression should also include the cyber warfare challenges especially emanating from the non-state actors and the new conceptions of territoriality will need to be taken into account by the International Criminal Court to institute a viable framework of accountability⁶. Schmitt who served as the director of the Tallinn project cautions that our understanding of how international law applies to cyber operations is in its infancy and many issues lack clarity or are the subject of important disagreement, which aspect needs to be borne in mind by state legal advisors so as to refine and develop the law governing cyberspace through state practice and expressions of *opinio juris*⁷. Schmitt also argues that states need to act as responsible inhabitants of cyberspace and should

¹Eric Boylan, *Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners*, Vanderbilt Journal of Transnational Law, 2017, Vol.50:217. Also see, Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 Berkeley Journal of International Law, 192 (2009)

²Antonia Chayes, *Rethinking Warfare: The Ambiguity of Cyber Attacks*, Harvard National Security Journal, 2015, Vol.6, pp.474-519.

³Kubo Macak, *From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law*, 9th International Conference on Cyber Conflict, 2017.

⁴Kilovaty, Ido, *Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare*, American University National Security Law Brief 5, no.1 (2014): 91-124.

⁵Carl Fitz, *All is Fair in Love and Cyberwar: International Law and Cyber-Attacks*, Houston Journal of International Law, 2017, Vol.1, pp.1-17.

⁶Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, Duke Law & Technology Review, 2010, No.3.

⁷Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum*, Harvard National Security Journal, 2017, Vol.8, pp.239-282.



lower the point at which cyber operations violate the prohibition on the use of force so to allow states to respond forcefully to non-destructive cyber operations and enhance the protection of cyber infrastructure, data and activities during armed conflicts¹. Iaria prescribes that states should move towards better regulation of cyberspace by marking the websites and servers with emblems or codes so that the distinction between combatants and civilians in war is easily discernible². Kodar argues that challenges such as ‘when is a cyber attack an ‘attack’ under LOAC and when is it only a hindrance’ do not warrant the rush into a new legal instrument, but can be defined in reality by the relevant state practice³. The question⁴ also remains whether countermeasures to cyber-attacks provide adequate protection to nations initiating them under the UN Convention? It is also felt that international legal options against terrorist cyber activities exist, but states lack the incentives to strengthen the applicable international law⁵.

India's Policy on Cyber Warfare:

India's Information Technology Act, 2000 is the mainstay of legal regime which governs the cybersecurity in our country, and to some extent by the Indian Telegraph Act, 1885 and the Indian Penal Code. Our country unveiled a comprehensive National Cybersecurity Policy in 2013 with the objective to build a secure and resilient cyberspace for citizens, business, and government. Under this Cybersecurity Policy, India envisioned major institutional structures to effectively deal with cybersecurity, viz. (1) the **Indian Computer Emergency Response Team** (CERT-In) which serves as the national nodal agency to deal with cybersecurity incidents. It collects, analyzes, and disseminates information on cyber incidents and coordinates with various cybersecurity agencies, issuing alerts, guidelines, and advisories; (2) **National Cybercrime Coordination Centre** (NCCC) oversees the execution of online cybercrime reporting and monitoring and is tasked with the setting up forensic units, building cybercrime handling capabilities in the police, prosecutors & judicial officials, and promoting R&D in the field of cybersecurity; (3) **National Critical Information Infrastructure Protection Centre** (NCIIPC) serves as the nodal agency to protect critical information infrastructure including telecommunication networks, online payment gateways, electronic stock trading, and digital infrastructure in air control and space and (4) **Cyber Swachhta Kendra** - Botnet Cleaning and Malware Analysis

¹Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, Stanford Law and Policy Review, 2014, Vol.25, pp.269-299.

²Adriano Iaria, *E-Emblems: Protective Emblems and the Legal Challenges of Cyber Warfare*, IAI Commentaries 18, 35, June 2018

³ErkiKodar, *Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I*, ENDC Proceedings, Vol.15, 2012, pp.107-132

⁴Eugenia Georgiadeset al, *Responding to Cyber Attacks on Critical Information Infrastructures*, 30. J. Marshall Journal of Information Technology & Privacy, L.3. (2013).

⁵David P. Fidler, *Cyberspace, Terrorism and International Law*, Journal of Conflict & Security Law, 2016, Vol.21, No.3, pp.475-493.



Centre: examines the malware and botnets that affect networks and systems to notify and enable cleaning and securing systems of end-users to prevent further infections. Other agencies are also being set up to tackle specific cyber domains such as CERT-Fin for the financial sector, National Technical Research Organization under National Security Advisor for technological capability building in cyber security. Penal provisions against cybercrimes are contained in the Information Technology Act and the Indian Penal Code.

India has not joined international treaties like the Budapest Treaty on International Cooperation on Cyber security and Cybercrimes which will deprive it of the opportunity to seek international cooperation to investigate cross-border cyber attacks¹. India is in number 23 position in the UN Global Cyber security Index, 2017 and this is not a very safe and cyber-secure position. Recognizing that Pakistani hackers have been able to deface and take down several Indian military sites and expose the classified data, India is planning to put in place a tri-service agency for cyber warfare by the creation of a Defence Cyber Agency to work in coordination with the National Cyber Security Advisor². The National Technical Research Organisation (NTRO) – established in 2004 in our country is a specialised technical research unit which comes under the control of the Prime Minister's Office and engages largely in intelligence gathering. The Indian Computer Emergency Response Team (CERT-In) was established in 2004 under the Ministry of Electronics and Information Technology which acts as the national central body for cyber incident response, while also facilitating cross-sector co-operation in cyber strategy. Experts suggest that transposing India's recent surgical strike attacks against Pakistan and Burma as a counter-measure for cyber-attacks would serve as a credible threat to adversaries who were planning to get away with low-intensity cyber-attacks³. It is apprehended that more than one billion Aadhar card data in India is prone for cyber-attacks, so much to say the Reserve Bank of India in its recent white paper has cautioned that the Aadhar data is readily available for the cyber-attackers⁴. In line with the same, when the 5-Judge Constitution Bench of our Supreme Court recently upheld the constitutional validity of the Aadhar law, at the same time, it struck down certain provisions of the Aadhar Act and also read down some of the provisions and prescribed stringent

¹Divij Joshi, *A Comparison of Legal and Regulatory Approaches to Cybersecurity in India and United Kingdom*, The Centre for Internet & Society.

²See <https://economictimes.indiatimes.com/news/defence/india-is-quietly-preparing-a-cyber-warfare-unit-to-fight-a-new-kind-of-enemy/articleshow/61141277.cms> as last visited on 30.10.2018

³ See <https://thewire.in/tech/india-needs-credible-deterrence-strategy-cyberspace> as last visited on 19.10.2018

⁴See <https://www.cybersecurity-insiders.com/data-of-more-than-1-billion-indian-aadhaar-cards-is-open-to-cyber-attack/> as last visited on 19.10.2018



standards for the safety of the data and its handling by private actors such as banks, financial institutions and telecom companies¹.

Conclusion

The recent innovations and rapid developments in areas like internet, mobile telephony, cloud computing, artificial intelligence, internet of things and the omnipresent e-commerce all place at the hands of a potential cyber-attacker huge data and inter-connected critical infrastructure systems exposing them to grave and imminent danger. The fact that technology has been able to rapidly develop well beyond international law on this subject is particularly true in relation to the cyber attacks and wars. In several instances of such attacks, they are usually given the treatment of a cybercrime and not of a cyber war. This is particularly true because the existing amorphous nature of the international regulations including the UN Charter, LOAC and connected conventions and international agreements do not prescribe an 'armed attack' in response to a 'cyber-attack' on a nation's critical infrastructure and still the victim states are relegated to apply only mitigative counter-measures like similar reprisals or sanctions and not engage in an armed retaliation. Although in principle international jurists opine that an armed response to a cyber war is justifiable, none of the victim states have so far unleashed them and the 'state practices' in this regard also do not lean in favour of a war response. Well beyond the 'denial of services' effect, jurists are increasingly looking at a more higher threshold of a 'crippling effect' of cyber-war attacks which last for a fairly long duration leading to a collapse of a part of a nation's system or facility or destruction of them or death and indiscriminate loss or injury of its citizens as circumstances which can warrant a victim state to employ the preventive 'self-defense' to initiate war against the perpetrating nation. Thus, the state practice and *opinio juris* on this subject at the moment do not lean in favour of initiating a full scale war against a country or a state which harbours non-state actors indulging in cyber warfare, especially when the above higher threshold and other principles of LOAC are not met and succinctly answered.

¹K.S. Puttaswamy and Others vs. Union of India and Others 5-Judge Supreme Court of India decision dated September 26, 2018.



A STUDY ON CYBER BULLYING WITH SPECIAL REFERENCE TO SCHOOLS AND COLLEGES

Ms. Harshavardhini P.,

B.B.A.LL.B. (Hons), Saveetha School of Law, Saveetha Institute of Medical and Technical Science, Chennai, Tamil Nadu
&

Ms. A. Udhaya Sweetline,

B.B.A.LL.B. (Hons), Saveetha School of Law, Saveetha Institute of Medical and Technical Science, Chennai, Tamil Nadu

INTRODUCTION

Cyber bullying is fast growing in this digital world among school and college Technology in the current phase is developing and there are changing on various ways of functions of the society. The term Cyber bullying means a person or group of people who involve in activities to bully, tease or make a person uncomfortable through phones or the Internet. Cyber bullying can cause immense damage to people in real word. Bullying victim face aggressive action from anyone who is dominant they are be bullied repeatedly and over many time exposed negative action action by students.social networks give public the ability to post photos of anything they need. Cyber bullies are take chance to conner certain person's life to harmful way .The technology has been used by lots of children that negatively affect the child's activities and become clearer about acts. The more time spent in online is been increased rapidly therefore children lose the social environment. Cyber bullying was define by Beasley "the uses of communication and information technology are like phone, messages, mails, defamatory website, and online polling website ,repeated and behavior of individual or group that are intended to cause damage are harm to others. It is act done by a person are groups who is either physically and social strong over their victims. It is to noted that harassers are under the age of 18 yr. as per the report it state that 50 % of children are been victims of cyber bullying in which others are been threatened. One of the reasons that cyber bullying has given more importance nowadays due to more cases of suicide of teenagers as results in incessant cyber bullying. There are many parents are working and provide expensive gadgets to their kids in order to compensate time because they may can't able spend with them. This backfire the parents were kids will misuse them. In most of report state girls are been vulnerable in case of bullying as sexual can be humiliating in open world. Traditionally in India parents alone is not responsible even schools are highly responsible for child.

Objectives

- To understand the concept of cyber bullying and its kinds.



- To trace the precautions and preventions taken by the school administration pertaining to this crime.
- To analyze the legal remedies under the Indian legislation for cyber bullying.
- To know the laws governing the issue of cyber bullying in other countries.

.Sources of study and Material

The researcher has referred to only secondary sources such as Journals, books, internet sources.

Scope of the study

The author in this paper has studied and focused on the crime of cyber bullying, cases pertaining to it and its legislations in India and few other countries.

Cyber bullying in India

According to Indian scenario nearly 8 out of 10 people are affected to various type of cyber bullying. Were out of these 60% on online abuse and rest all false rumors for degrading the image. Schools and Colleges students are been related to some part of bullying and cyber bullying. The study state that India as country facing the largest cyber bullying than other countries .there is a increasing cases of cyber bullying in India were the "the ministry of women and children has launched helpline to report cyber bullying cases .

Cyber bullies are teenage they lack sense of understanding of their action and it consequence on others. The main reason for bullying is frustration, irritation, weariness of bullies. The fact that course will be long lasting clash on person been bullied. Generally bullies will have strong mind to take revenge .if any person who can't able to speak directly will take tool of cyber bullying .there are many reasons like socially and physically powerful.

India laws are not been effective towards problem of cyber bullying. The cases are been gradually increasing day by day and reached the third position on cyber bullying cases all over the world. The regulation related concern on information technology act 2000 with amendment of 2008. The main drawback is IT act does not touch upon matter related to offences and threat on cyber bullying.

Kinds of cyber bullying

There are various kinds of cyber bullying. To name few are those been involving personal information of persons like photos etc. Destroying the person information through viruses, images through phones are some kinds. Others kinds of bully engages in revealing a person secret, rude comment harassing, misusing data, misuse passwords, other polling. There are many modes to bullying someone is text messages, mails, gaming intention to cause person threat, defaming, sexual harassment, rumors and gossip etc. Most popular type is fake account, games, abusing someone.



Cyber bullying on schools and its Implications for school Policy

After rigorously reviewing the language from several state laws and recent cases, we tend to advocate for primary elements of what would represent a good school policy. They embody the following:

Schools have to be compelled to educate students in a way to handle bullying. It absolutely was found that 57 % of the cyber bullying was out of revenge, whereas 41 % of the time it absolutely was out of anger. Within the data, some students urged to "just ignore it" and hope it goes away. Before colleges will expect teenagers to own "netiquette", victimization the net properly, and treat others well, they have to be school acceptable non-harassment behavior. Within past number of years, programs and resources are created out there on however colleges will modify cyber bullying additional data regarding these resources must get into the hands of parents and educators.

The main important issue is victims are not informing teachers, parent or others of the cyber bullying. In the case of Ryan Halligan the 13 yr old who took his life stated that there is need to develop the awareness of parent and others.

1. Specific definitions of harassment, intimidation, and bullying (including the electronic variants)
2. Graduated consequences and remedial actions
3. Procedures for reportage
4. Procedures for investigation
5. Language specifying that if a student off-campus speech or behavior ends up in substantial disruption of the learning atmosphere or infringes on the right of other students, the student is disciplined.
6. Procedures for preventing cyber bullying

Other than being dependent on technology for prevention of cyber bullying, teachers, parents, and students themselves have to be compelled to take measures to prevent such offence. There is advertisements on the results of cyber bullying and its thought. Anti-ragging cells and additionally posters within the school will facilitate to prevent it.

School authorities ought to build students perceive the thought of cyber bullying, its consequences and effects. They ought to teach cyber ethics to the students and impart data of laws against cyber bullying. Faculties will forestall identical by organizing some activities or interactive sessions to allow them the complete plan of cyber bullying. Faculties ought to additionally embrace within the policy, their right to interfere in actions of a toddler off-campus that affects the youngsters' on-campus too. There ought to even be a lecturer within the faculty, a counsel-or who will consider the matter of cyber bullying and facilitate the victim to cope up with it. Faculty ought to additionally monitor the net activities of the scholars and will



take necessary disciplinary actions against identical. Oldsters ought to justify students what's cyber bullying, ought to facilitate their kid if he has become a victim of identical.

Parents should keep a check on the net usage and activities of their kid. They ought to additionally build some rules within the house associated with net usage. They ought to maintain healthy relations with the kid and will encourage the kid to inform them if they're being browbeaten. they ought to additionally save evidences and guide the kid on what he keep him busy and additionally inspire him regarding positive things. They ought to build criticism as shortly as doable. Parents ought to inform the college authorities additionally. They will additionally look for protection from the court by filing a case.

Legal remedies

The Indian legal framers have provided remedies for cyber bullying under the Information and Technology Act, 2000 and the Indian penal code, 1860.

Prior to the 2008 amendment of the Information and Technology IPC was governing the offences happening in the cyber world in relation to harassment, stalking, defamation, insult and intimidation.

Information Technology Act:

Section 66A which came into existence after the amended IT Act provides remedies for the crimes for cyber bullying where the offender is punished for a period upto three years with fine for sending any messages with the medium of computer or any electronic devices that is grossly offensive or any communication which he/she knows to be false, but in order to cause insult, annoyance and criminal intimidation.¹

Section 67 prescribes that any person publishing or transmitting through electronic form any obscene material is punishable for a term which may extend to five years and also with the fine which may extend to ten lakh rupees.²

Section 66 E provides punishment for violating privacy of any person by capturing, transmitting or publishing private and confidential pictures of other the punishment shall be imprisonment up to three years or fine up to three lakhs.³

Indian Penal Code

Section 507- In the cases of criminal intimidation through an anonymous communication is punishable for imprisonment up to two years.⁴

Section 354D - under this section stalking is under the purview of offence is punished with three years of imprisonment and fine under first conviction and imprisonment for up to is five years for subsequent offender.¹

¹ Information Technology Act, 2000; §. 66A.

² Information Technology Act, 200; § 67.

³ Information Technology Act, 2000; §66E.

⁴ Indian Penal Code, 1860; § 507.



Recent cases related to cyber bullying:

Layshock v. hermitage administrative district (2006)

A student created a web site from his grandmother's information processing system making a parody of the college principal on his myspace.com. Whereas the positioning was non-threatening and created off-campus, college officers were ready to prove a serious disruption to the college day. Officials found out those workers devoted a lot of additional time dispersive and partitioning the case. Secondly, the pc system had to be clean up, leading to off categories and disrupting the academic surroundings.²

Jessica logan case

Jessica logan case of cyber bullying, wherever the implications led to suicide of the victim was of Jessica logan. Jessica was an eighteen year old school lady who had sent nude photos to her love. The lover shared those photos due to psychological hurt, depression, low shallowness, isolation, anxiety, low grades, and frustration. Cyber bullying research facility has termed the development of suicide that is in cyber bullying.³

Other than the psychological hurt to the victim, there will be legal consequences against the bully too. The legal consequences will be either criminal or civil and therefore the bully may well be tried for constant. As penalization, the consequence will be expulsion or suspension from faculty or faculty. The costs will be that of defamation, threat, theft, outraging the modesty of a girl, harassment, etc.

Ritu Koli Case

Facts:

The fact that cyber stalking doesn't involve physical contact could produce the misperception that it's additional benign than physical stalking. This is often not essentially true. Because the Internet becomes an ever more integral a part of our personal and professional lives, stalkers will profit of the benefit of communications yet as hyperbolic access to private info. Whereas a possible stalker is also unwilling or unable to confront a victim in the flesh or on the phone, he or she could have very little hesitation causation harassing or threatening electronic communications to a victim. Like physical stalking, online harassment and threats is also a prelude to a more serious behavior, together with physical violence.

¹ Indian Penal Code, 1860; §354D.

² Matthew Beatus, Layshock ex rel. Layshock v. Hermitage School District, New York Law Review, Vol.56, Issue 2011/12, at pg.no 790.

³ Cyber bullying, socialna-akademija, <http://socialna-akademija.si/joiningforces/category/joining-forces-to-combat-cyberbullying-in-schools/chapter-3-cyberbullying/>



Decision

The Delhi Police has registered India's 1st Case of Cyber stalking in 2001¹ wherever a girl named Ritu Kohli complained that an individual WHO was victimization her identity to speak over the web at the web site World Wide Web.mirc.com was additionally deliberately giving her signal to alternative chatters encouraging them to decision Ritu Kohli at odd hours. As a result of that, Mrs. Kohli received an estimate of forty calls, national yet as international, throughout odd hours inside three days. A case was registered under section 509 of the Indian legal code (Word, gesture or act meant to insult the modesty of a woman).

Rithika Sharma Case

Facts

Ritika Sharma (name changed), WHO studies at a prominent Delhi school, visited the police once being stalked by a Face book user whom she had befriended on the site a month ago.

She had given her cell phone range to the person WHO was later found to be employing a pretend name, image and signal.

Experts say cyber bullying and cyber stalking are progressively changing into a daily downside for the city's School kids with individual's victimization transmission like emailing, social networking and texting to harass or pursue them. Decision Delhi Police has been launching cyber safety awareness programs in colleges within which students are familiar to avoid giving personal info on-line to anyone they do not grasp.

Cyber bullying in other countries

USA - In order to curb the offence and crime of cyber bullying various states have passes and implemented legislation. While there are no federal laws as of now pertaining to the above mentioned crime.

Canada -The cyber bullies are suspended from schools and in cases of repeated offender he/she has to undergo expulsion and jail time for the act done under the Education Act.

United Kingdom -The person engaged in cyber bullying under the Malicious Communications Act shall be punished for a period of six month are more in jail and along with a huge number of fine.²

The laws governing cyber bullying are:

Protection from Harassment Act 1997,.

- Criminal Justice and Public Order Act 1994.
- Malicious Communications Act 1988.

¹Mukut, Cyber Stalking - A "Virtual" Crime With Real Consequences, worldpulse, (November, 05, 2015)<https://www.worldpulse.com/en/community/users/mukut/posts/22772>

²Cyber bullying laws around the globe: where legislation is strongest?, UKknownkids, (October, 16, 2014, 7:56pm), <http://resources.uknowkids.com/blog/cyberbullying-laws-around-the-globe-where-is-legislation-strongest>



- Communications Act 2003.
- Breach of the Peace (Scotland).
- Defamation Act 2013

Philippines -The school has the responsibility to comply with the Republic Act 10627 and has to implement and eradicate cyber bullying through the means of policies in schools and in case of non compliance by the school authorities sanctions is levied on them through the act.

Australia -The laws in each territory take three forms: Actions by state, lawsuit by the victim, and "Articulate of Industry Codes."Federal Nature of Law, cyber bullying laws varies from territory to territory.

Conclusion

In this fast pacing world cyber bullying is an ongoing issue. The bully can be a person or group of individuals from old to a teenager. The victim of cyber bullying at a larger group are teenagers especially girls. They are threaten and harassed through emails, messages, gaming websites and other online platforms. Victims are scared that they often do not tell the problems they are encountering or facing by this type of bullying.

The legal framers have to make stringent laws and punishments to curb this issue as these crimes are instigating the teenagers to end their life. India has to take this issue seriously and the trend of memes is also a way of cyber bullying. The meme creators are to be stopped from making memes and all contents of cyber bullying is to be removed from the internet by appointing a special commission for it as usage of internet cannot be stopped in the present era.



PSYCHOLOGY AND CHILD PORNOGRAPHY- A COMPARATIVE STUDY

Richu Theresa Robert,

III B.A.LL.B., Government Law College, Thiruvananthapuram, Kerala.

&

Kavya Y.S.,

III B.A.LL.B., Government Law College, Thiruvananthapuram, Kerala.

INTRODUCTION

In a famous speech, former US Supreme Court Justice Oliver Wendell Holmes once said, "It cannot be helped, it is as it should be, that the law is behind the times". In this era of digitalization, law in its strictest sense, cannot remain stagnant. Law has to evolve with the changing times. People find various ways to defy law and there are various avenues available to ensure that the rule breakers are not brought to justice. In a time when being 'online' matter more, the group that is more affected by the lack of definite laws on cyber space are children.

Child pornography on the internet is one of the most prevalent crimes in the world that involves technology. Federal law defines child pornography as any visual depiction of sexually explicit content involving a minor. Years ago, child pornography was when a child was depicted in a sexual way in a photograph or paintings. However, with the advent of technology, the spread of child pornography via the internet and mainly the dark web has become a common practice.

The growth of internet has been hugely beneficial to many industries across the world. However, lack of proper laws safeguarding the privacy of the content available online paves way for the offenders to take disadvantage of the information online. As child pornography depicts children who are below the age of 18, there is no element of consent that should keep in mind. Production and circulation of child pornography on the internet is easy, which proves difficult for the law enforcement to take notice of it and take it down.

In this paper, we intend to compare the various laws that are involved in stopping the spread of child pornography across the world, while comparing the effects of Section 67 and 67B of Information Technology Act 2000 in stopping child pornography in India. We delve into the deeper psychological state of the victims and their victimization in the cyber space as the information once entered into the internet is not entirely taken down. Our chief goal is to examine how the cyber laws can be evolved to ensure the eradication of the evil of child pornography.



EVOLUTION OF LAW AGAINST CHILD PORNOGRAPHY IN INDIA

Child pornography is a heinous crime whose evolution is not a new concept. It has existed for a long time. However there was no proper definition as to what child pornography means. Indian Penal Code previously had not proper punishments mentioned for the offence of child pornography. This changed during the landmark case of *Sakshi v. Union of India*¹ where Sakshi, an organization for the upliftment of women filed a Public Interest Litigation that the trend at that time was sexual abuse against children and women other than penile penetration, which would not come under the purview of Section 375/376 of IPC. The Law Commission filed an affidavit confirming the views expressed in the 156th Law Commission Report² dealing with the concerns raised in the writ, only with certain minor changes. However, the Supreme Court was inclined to agree with the submissions made in the writ and as a result, 172nd Law Commission Report³ has reviewed all laws and sections 354, 376 and 377 which dealt with sexual offences were also applied to sexual abuses of children. However, even these provisions were not adequate for cases relating to children. The amendments brought after the *Nirbhaya case*⁴ did help to a certain extent, but even then there were issues in the law dealing with offences against children.

Previously, obscenity was dealt by Sections 292 and 293 of IPC. However; online obscenity was not covered under this section. This was solved by the inclusion of Section 29A, which included electronic documents applicable to obscenity. Section 35 puts knowledge or intention to be proved on the part of the parties, which is difficult in the case of Internet Service Providers. In certain cases, Supreme Court differentiated “Pornography” and “Obscenity”. While both offend public morality and decency, pornography is obscenity in a more aggravated form. In online pornography, especially that of children, clause (1) of Section 292 does not hold much weight as proving of intention and knowledge would tip the balance in favor of the offender.

It is important to know that the Information Act 2000 played a big role in forming the earlier legislation regarding online pornography. However, there was no specific mention of child pornography as such, only that of pornography under Section 67 of the Information Act 2000⁵

The transmission or publishing of obscene materials is punishable by imprisonment of two years and fine which may extend to five lakh rupees and second conviction is punishable by imprisonment of five years and fine which may extend to ten lakh rupees. The offence made under this act is non bailable and cognizable. Also Section 67C imposes liability on intermediaries for the retention and production of information. Section 79 was also amended. It

¹ *Sakshi v. Union Of India*, A.I.R 2004 SC 3566

² 156th Law Commission of India Report, Offences against women and children, available at <http://lawcommissionofindia.nic.in/101-169/Report156Vol1.pdf>

³ 172nd Law Commission of India Report, Review of Rape Laws, available at <http://www.lawcommissionofindia.nic.in/rapelaws.htm>

⁴ *State Through Reference v. Ram Singh and Ors.* 13th March 2014 <https://indiankanoon.org/doc/57145403/>

⁵ Akshay Sapre, Commentary on Information Technology Act, 241-247 (3rd ed 2016)



specifies the conditions under which liability will not be imposed on intermediaries. It provides a confusion regarding the liability of cybercafé owners on what is being watched or browsed on the internet in their establishments. Their grounds of defense can be made stronger by the application of powerful software and other technology that prevents the patrons from viewing pornographic sites. If they do overcome these restrictions those who do it will be liable and not the cybercafé owners.

In 2008, the Information Act was amended and included Section 67B which specified the areas of production and circulation of child pornography and the punishments for it which is imprisonment of either description extending to five years and fine of ten lakhs on first conviction and imprisonment of either description of a term extending to seven years and also a fine extending to ten lakhs on second or subsequent conviction, provided that the publication of the content is in digital form and is not a part of heritage and religious beliefs. The PIL filed in *Janhit Manch v. Union of India*¹ called for a blanket ban on pornographic content. The organization argued that pornographic content, especially child pornographic content on these sites leads children and youth in a delinquent path and plays a role in the formation of future criminals.

The expression '*publishing and transmission*' has not been specifically defined under the IT Act. But in *Taxman's Commentary* under the IT Act, *publishing* means '*making information available to people*'. The Commentary also states that transmission and not mere possession of pornographic content is not an offence. But it is to be noted that in the case of child pornography, both possession and transmission of the pornographic content is a punishable offence.

The increase in crimes against children is in a way a cause for the increase in child pornography in India. This increase in child crimes has led to the advent of The Protection of Children from Sexual Offences Act or the POCSO Act. The Act came into force on 14th November 2012. This Act criminalizes sexual assault, harassment and child pornography. This Act lays down guidelines for the police and court authorities to deal with the victims. It gives specific punishments to specific crimes. Special courts are established to deal with cases under the POCSO Act. The Act prescribes stringent punishments graded as per the gravity of the offense with the maximum term of rigorous imprisonment of life and fine. Chapter 3 of Protection of Children from Sexual Offences Act defines using child for pornographic purposes and punishments therefore defined in Sections 13, 14 and 15. Section 13 defines using child for pornographic purpose, Section 14 defines punishment for using child for pornographic purposes and Section 15 defines punishment for storing pornographic materials involving children. But the question of how far this Act is effective in establishing such specific guidelines is a cause for concern.

¹ Janhit Manch and Ors v. The Union of India, PIL No.155 of 2009, 10 March 2010



INTERNATIONAL INSTRUMENTS TO CURB CHILD PORNOGRAPHY AND ITS NATURE

- Optional Protocol to the CRC on the sale of children, child prostitution and child pornography (OPSC)-Child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes
- Council Of European Convention on Cyber Crimes('Budapest Convention')-
- Council of Europe Convention On The Protection Against Sexual Abuse ('Lanzarot Convention')
- EU Directive 2011/92/EU-A child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes¹

COMPARING THE LEGAL PERSPECTIVES OF COUNTRIES ON CHILD PORNOGRAPHY

In American Federal Law, Section 2256 of Title 18, United States Court, defines child pornography as any visual depiction which may include photographs, videos, digital or computer generated images indistinguishable from an actual minor, and images created, adapted or modified, but appear to depict and identifiable, actual minor. Undeveloped film, undeveloped video tape and electronically stored data that can be converted into visual image of child pornography are also deemed illegal visual depiction under federal law. In American law, a picture of a naked child may constitute illegal child pornography if it is sexually suggestive. Also, the age of consent in the federal states is 18 years. However, any video or online pornographic content of any person under the age of 18 years is punishable, irrespective of the element of consent. The current US State statute makes it illegal to persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for purpose of producing visual depictions of that conduct². Any individual who conspires to commit a child pornographic offence is also subject to prosecution under federal law. Any violation of federal child pornography law is a serious crime. For eg; First time offender convicted of producing child pornography under 18 U.S.C. 2251, face fines and statutory minimum of 15 years to 30 years maximum in prison³

According to the American law, computer generated sexually explicit images of children are not illegal. However; India has not adopted this law. In India, computer generated sexually explicit content of children is a punishable offence.

The distribution of child pornography online is mainly done via internet websites and the dark web. Some argue that due to the stringent cyber laws and policing of ISPs result in curbing of the circulation of online child pornography. However the fact remains that the production, distribution and circulation of child pornographic content is an ever increasing problem. One strategy of distributors is to post temporary sites that are then advertised on pedophile bulletin boards. To prolong their existence these sites may be given innocuous names (e.g., volleyball) or

¹ Prof. Alisdair Gillespie, Lancaster University of Law

² 18 U.S.C. 2256 [8].

³ 18 U.S.C 2251-Sexual Exploitation of Children (Production of Child Pornography)



other codes (e.g., ch*ldp*rn) to pass screening software. The websites may be immediately flooded with hits before they are closed down. Often the websites contain Zip archives, the password for which is then later posted on a bulletin board.¹

The Pakistani statutes had no mention of child pornography in any way or form. However, following the pedophile scandal in August 2015, the Pakistan Penal Code was amended through Criminal Law Second Amendment Act 2016 in April 2017 to address the serious issues of child abuse. Section 82 of Pakistan Penal Code was amended and age of child was enhanced from 7 to 10 years. In Pakistan, anyone under the age of 10 was considered as a child. Three new sections were added to the Pakistan Penal Code in which 292Bis about the offence of child pornography and 292C is about punishment of child pornography.

Protection of Children Act 1978 in UK was passed in response to the growing problem of child pornography. Its main purpose was to close some potential gaps in the measures available to police and prosecutors. The definition of “photograph” given in Section 7(4) of the 1978 Act was extended to include photographs in electronic data format following the amendments made by Section 84(4) of the Criminal Justice and Public Order Act 1994. The CJPOA 1994 introduced the concept of ‘psuedophotographs’ of children. Psuedophotographs are technically photographs but they are made by manipulating an existing picture using a computer software. It is now an offence for a person to “take, permit to be taken or to make, any indecent photographs or pseudophotographs of children or distribute or show such indecent photographs or pseudophotographs” under Section 1 of the 1978 Act.²

The European Commission launched a communication paper on ‘Illegal and Harmful Content’ together with the Green Paper on the Protection of Minors and Human Dignity in Audio Visual and Information Services in October 1996. The Communication Paper was the result of calls for the regulation of the Internet within the European Union dating from early 1996. The European Commission documents followed a resolution adopted by the Telecommunications Council of Ministers in September 1996, concerning the dissemination of illegal content on the internet, especially child pornography. The Green Paper sets out to examine the challenges that society faces in ensuring that these issues if overriding public interest are adequately taken into account in the rapidly evolving world of Audio Visual and Information Services. All these initiatives at the European level were adopted in a Resolution at the Telecommunications Council in November 1996.

DARK WEB; A MENACE?

Dark web is the inaccessible part of the World Wide Web that can only be accessed by specialized individuals using special software. No one can access dark web from ordinary search engines. It is like an onion, which has to be peeled layer by layer to reveal its inner part. Dark

¹Richard Wortley and Stephen Smallbone, Child Pornography On The Internet, No. 41, 11 (2010)

²Dr. Atik-ur-Rahman, Online Child Sex Abuse, pg 44-58 (1st ed 2013)



web is accessed by Tor, which stands for the 'Onion Router'. This encourages anonymous communication. Dark web is also known as the 'Deep Web'. Dark web is the breeding ground for illegal activities like terrorism, illegal transactions and of course, online child pornography.

Technically, both the Dark Web and the Deep Web are legal. There are many websites that exist within the Dark Web that provide illegal products or services. But generally speaking, the Deep Web and Dark Web in and of themselves are legal. Cyber experts say that some FBI offices in the US go undercover on the Dark Web to keep track of illegal activities. In India, there have been at least two cases in the past year in Chennai and Mumbai where LSD was purchased on the Dark Web using Bitcoins.

PSYCHOLOGY OF THE VICTIMS OF ONLINE CHILD PORNOGRAPHY

The victims of online child pornography can be seen as different from that of victims of other sex crimes. The effects of the victims can be classified into two, the immediate effects and the long term effects. The immediate effect may include physical illness, mental stress, anxiety, Post Traumatic Stress Disorder (PTSD), nightmares etc. Long term effects on child victims include depression, anxiety, Post Traumatic Stress Disorder, risky behavior; self-mutilation, suicidal attempts, ongoing humiliation and lack of privacy¹. The victims constantly fear the burden of the pornographic content and keep thinking that anyone they know might have viewed the images online. This fear makes them to be introverts and they do not have the courage to be self-reliant or have any confidence about themselves. Even in their later years, victims of child pornography grow up into shy adults with no self-confidence. They constantly worry about the images that they are sure exist online and worry if someone would recognize them, forcing them to not be in a stable relationship in their life. They might have difficulty in their relationships, careers and other stages of life. People who struggle with the victim mentality are convinced that life is not only beyond their control, but is out to deliberately hurt them. This results in constant blame, finger pointing and pity parties that are fuelled by pessimism, fear and anger.

The internet plays a huge role in the victimization of children and later, revictimization of these children as adults. In this age of technology, it is impossible to stay detached from internet connectivity. And we know how difficult it is to get rid of something once it is online. Evils like child pornography obviously would have remnants online, no matter how hard people try to get rid of the evidence. It is also a huge factor in how the victims of child pornography become victimized again. The fear that someone they know has seen these pornographic images prompts them to make sure that these people do not speak about it. As a result, these children to a certain extent are abused again and maybe made to do sexual favors for them in exchange for their silence, further deepening the web they are trapped in.



The mental condition of the victims of child pornography is devastatingly painful. According to experts in penalizing child pornography, the initial reaction of the children who are subjected to online child pornography is silence. This silence is said to be deafening and uneasy. These children tend to blame themselves for their fate. Children remain silent and refuse to disclose the abuse that happened to them. Psychologists say that this silence conveys their sense of helplessness¹ which is clearly understood from their reluctance to report the incident. This helplessness comes from a breach of trust, as the fact that the abuse was done by someone they knew and trusted. The images of their abuse are recorded and distributed online, which is in circulation in the internet. It is a horrifying fact that online child pornography, to a certain extent originates from the very people that a child trusts—a parent, a teacher or a parent. Victims are eroticized by parents under the guise of ‘modeling’ and then have sold images online as ‘solo pornography’.² In some cases, the victims might have been engaged in consensual sexual relationship. However, after a breakup, their photos and videos, which were captured in secret and with trust, are published online, with an aim to destroying the credibility and reputation of the person shown in the image. This practice is done as revenge and is seen among teenagers as an emotional response to breakups in relationships.

Once these children come to the realization that their pornographic images are available online, it creates panic and anxiety, not to mention a sense of shame that would drive them to do grave things. In this technological age, it is easy to find these kinds of images online. Even with the technologies nowadays, it is easy to match newly discovered pornographic images online, thus enabling them to connect the images to old and new cases. But even with advanced technologies, not every child can be discovered. The perpetrators often get rid of all the evidence pointing to them. Thus there remains no other way to track the masterminds behind this heinous crime.

Another psychological aspect of a small fraction of victims of child pornography online is that the children who were abused and whose images are circulated in the form of child pornography tend to become more open while discussing the abuse they faced and about the sexually explicit content produced. However, this proved to be a hindrance as the prosecution lawyers often accuse the child of fabricating stories to destroy the reputation of the accused person. The victims of such abuses and exploitation are rarely candid. But there is certain exception to these kinds of cases. This poses a problem in trials of sexual abuse and pornography as the child, with repeated interviews which is necessary in a criminal investigation and trial, the child becomes more experienced and does not have any problem

¹ Sarah Chang, “I watch child pornography to prosecute sex crimes. The kids' silence is deafening”, WP October 23 2015

² Wendy Walsh, Janis Wolak, The complex experience of child pornography survivors, The Intl.Journ, September 2018



in narrating the incident again and again. With this, they call prey to the accusation that the children have been coached. It gives an opportunity for defense lawyer to question the credibility of the child. It is easy to claim that any evidence given by the child is fabricated and the child is coached, based on the fact that the child appear to be cool and calm, as compared to how a child victim of abuse and child pornography usually reacts in such situations.

The psychology of victims of child pornography varies from victims to victims. Throughout history, many psychologists were fascinated with how children grew up to be adults with psychopathic tendencies. In 1830s, these people, who the psychologists claimed were those with moral insanity, were believed to have grown up from children who had violent tendencies from an early age. In 1976, in the book 'The Mask of Sanity', Hervey Cleckley popularized and standardized the term *psychopath* to describe a person who lacks all conscience. A key characteristic of psychopathy, said Cleckley, is inability to feel normal emotion. Psychopaths are incapable of not only remorse, but also of shame, guilt, empathy for others, distress, and anxiety and fear in the face of punishment. Because they lack emotional connections to others, they often behave cruelly and irresponsibly. Their behavior, said Cleckley, is impulsive; psychopaths behave callously more for the thrill than for personal gains. If they are caught in a lie, psychopaths pretend to feel remorse and promise to make amends, but the truth is, they tend to hide their true intention. Psychopaths appear to be very charming and appealing to all those around him, but this same charm is used to manipulate those around him and get them to do his bidding even without them realizing that they are being manipulated.

There are two kinds of psychopaths. The first kind is cruel and is ruthless and won't hesitate to kill even a child. For them, the thrill of the chase and the hunt is more satisfying than anything else in the world. They kill when they feel like killing, even for the fun of it. The second is that of a more mellow kind. They tend to manipulate others to achieve gains in their economic status and careers, allowing them to further themselves into a better life. They might not have a penchant for trouble and are not usually bloodthirsty.

The psychopath's inability to feel emotional arousal-empathy, guilt, fear of punishment and anxiety under stress-suggest some aberration in the central nervous system. Indeed, psychopaths do not react physiologically to the threat of punishment the way other people do; this may be why they can behave fearlessly in situations that would scare others to death. Normally, when a person is anticipating danger, pain or punishment, the electrical conductance of the skin changes. A classically conditioned response that indicates anxiety or fear. But psychopaths are slow to develop such responses, which suggest that they are unable to feel the anxiety necessary for learning that their actions will have unpleasant consequences. Their lack of empathy for those suffering also seems to have a physiological basis. When psychopaths are shown pictures of people crying and in distress, their skin conductance barely shifts, in contrast to that of non-psychopaths, which shoots up. This emotional flatness may help distinguish



psychopaths from other aggressive people with anti-social personality disorder. Another trait of psychopaths is impulsivity, an inability to control responses to frustration, leads to breaking rules and laws may have a biological basis. Many psychopaths have abnormalities in the prefrontal cortex, which is responsible for planning an impulse control. For eg; on PET-Scan study found that cold blooded “predatory” murderers had less brain activity in the frontal lobe than did men who murdered in the heat of passion or controls of those who have not murdered anybody. One of the reasons for frontal lobe abnormalities may be brain damage resulting from physical neglect, accidents, battery, injury or emotional trauma and abuse.

Another psychological response that is commonly seen in victims of child pornography is a sense of shame and powerlessness. The knowledge that their pornographic videos and images are online; clearly visible for the entire world to see, no matter how well hidden it is in the web. In a 1990 study of 10 young child victims of sex rings that involved pornography, researchers noted that being photographed while being sexually abused exacerbated the victims’ experience of shame and humiliation (Hunt and Baird 1990). In a review of victims identified in several child pornography cases in Sweden, all of the children described how a sense of shame and guilt predominated their feelings at the time of disclosure of the abuse (Svedin and Back 2003). In the case of online child pornography, the sense of shame is deeper as their images, that is captured in various forms of sexual abuse is shown before the entire world. They are filled with shame as they think that everyone they know has viewed these images online and spreading them. This sense of shame is then changed to guilt when they think that people close to them, including family members would have seen these images and video, which causes pain and shame to them. Especially in Indian families, the topic of pornography is a taboo. In such a scenario, it is obvious that online child pornography is sensitive topic. It puts unnecessary pressure on the children, who feel that they have a duty to protect the reputation of their family. With their pornographic images being circulated online, they feel that they have betrayed their family, which drive these children to depression, and in more extreme cases, suicide. Victims depicted in child pornography were continually traumatized when they think of how many people were looking at their images on the internet at any minute of the day. They are consumed by the realization that they did not know anything about the identity of those viewing the images and had a general feeling of being unsafe, sexualized and victimized. To them, everyone is a potential perpetrator. They become withdrawn, unable to socialize and are reluctant to venture outside. Once these victims realize the permanency of these images, usually in their teens or adult years, they feel a loss of control, powerlessness, helplessness, shame and fear. This feeling of powerlessness follows them thorough their entire life, making their life difficult. In a way, they are revictimising themselves when they give the control of their life to others. These children grow up into adults with little or no self-confidence, which makes others take advantage of them in different ways. Once these children become aware about the presence of



their pornographic images online and realize that people have seen them, they are worried about who might have seen it. It is easy for someone to take advantage of these children sexually, in exchange for their silence. This only further damages the child in ways unimaginable to us.

MEASURES TO CURB ONLINE CHILD PORNOGRAPHY IN INDIA

From all the facts mentioned above, it is very obvious that online child pornography is a grave danger to the very existence of a healthy future generation. Only children who grow up into adults with confidence and sure of themselves become better citizens of the country. In order to ensure the future of our country, it is necessary to curb the spread of online child pornography in India.

It is true that the POCSO Act and Information Act 2000 have many provisions that have been effective towards curbing online child pornography in India. However the sad fact is that even with so many restrictions, online child pornography is still prevalent in India. Section 13, 14 and 15 of the POCSO Act clearly defines the law and punishments for child pornography in India. Section 15 defines punishment for storing pornographic materials involving children. However; it remains to see how far these laws are really effective in curbing child pornography online. Even after being caught on these charges, the loopholes are sufficient for the culprit to escape from punishment on minor technicalities. POCSO Act 2012 suffers from many flaws-non reporting of sexual abuse cases in most cases due to shame and the fear that the images and videos taken will be distributed online, police officials and administrative personnel remain aloof to these genuine concerns of the victims. Similarly, Section 67B of Information Act 2000 defines punishment for publishing or transmitting materials depicting children involved in sexually explicit act in electronic form. Even in this, specifications are blurry and many loopholes can be found which provides an easy way out for the culprits.

In a way, we can conclude that although there are measures in our legal system to curb online child pornography, it is still incomplete in many ways. The legislature, executive and judiciary has to work together to make more stringent laws that are effective in curbing online child pornography.

In this advanced age, it is easy to access dark web through onion routers, as a result of which people are able to move anonymously without the fear that their IP address will be discovered. These prompt pedophiles and other abusers to go into the dark web in search of child pornography. It is a sad fact that even with such advanced technology readily available to us in all size and forms; we are unable to discover something simple as an IP address. Internet Service Providers are not liable under law to provide any information regarding the perpetrators of these crimes. We can employ the expertise of the professionally skilled but unemployed youth of our country to develop technology to discover the IP address of those evading from the



spotlight, while involved in anti-social activities online, not just of child pornography but other crimes like terrorism and online frauds.

In a country like India, where 12.4% people still living in poverty and about 462 million people have access to internet, we do have a lot of offences related to internet, especially the misuse of innocent children trapped by the wide world that is available to them via the internet. Steps have to be taken by the government and the school managements to ensure that the children are properly educated about the threat that is hidden in the internet. Proper awareness is necessary to educate teenagers and children about cyber laws and how the Information Technology Act 2000 and POCSO Act can help them. Majority of the issues come from the fact that people are not aware about the laws that are in place to effectively fight online child pornography in India.

CONCLUSION

In the 72 years since India's independence, we have come a long way in both advancement of technologies and the development in our legal systems. The current systems in place are effective to a certain extent. But we have to realize the shortcomings in our present system and come up with more effective and novel ways to battle the misuse of technology. Stricter cyber laws is the need of the hour, considering the fact that we keep inventing new pieces of technology every single day and each of this technology has the power to make or break the nation. It is up to us to only focus on the better parts of the technology and make this country a safe haven for our children so that they grow up without fear and apprehension.



RIGHT OF PRIVACY AND DATA PROTECTION

Prasudha S.,

*IV B.A.LL.B. Integrated 5 Years Course , Kerala Law Academy,
Law College, Peroorkada, Thiruvananthapuram, Kerala*

&

Chithra B.,

*III B.A.LL.B. Integrated 5 Years Course, Kerala Law Academy,
Law College, Peroorkada, Thiruvananthapuram, Kerala*

INTRODUCTION

Data protection and privacy rights are two of the most important rights conferred by any civilized nation. Every individual and organisation has a right to protect and preserve her/its personal, sensitive and commercial data and information. The world privacy has been derived from the Latin word “Privatus which means separate from rest”. We have general laws and some of the provisions of these laws can be applied to data security, data protection and privacy protection in India. However, that is a temporary solution and in the long run we need dedicated privacy rights, privacy laws and data protection laws in India. Further, in this information technology era a special attention must be paid to the privacy rights in India in the information age. With the growing use of information and communication technology (ICT), data protection requirement has become very important. It would not be wrong to assume privacy and data protection rights as integral part of human rights protection in cyberspace.

PRIVACY PROTECTION AND DATA PROTECTION:

Privacy and data protection require that information about individuals should not be automatically made available to other individuals and organizations. Data protection is legal safeguard to prevent misuse of information about individual person on a medium including computers. It is adoption of administrative, technical, or physical deterrents to safeguard personal data. Privacy is closely connected to data protection. An individual's data like his name address, telephone-numbers, profession, family, choices, etc. are often available at various places like schools, colleges, banks, directories, surveys and on various web sites. Passing of such information to interested parties can lead to intrusion in privacy like incessant marketing calls. The main principles on privacy and data protection enumerated under the Information Technology (Amendment) Act, 2008 are defining data, civil and criminal.¹

RIGHT TO PRIVACY UNDER INDIAN CONSTITUTION:

The Indian Constitution do not expressly grants the right to privacy but this can be inferred under Article 19 (Freedom of Speech and Expression); Article 21 (Right to Life and

¹ http://14.139.60.114:8080/jspui/bitstream/123456789/12241/1/026_Privacy%20and%20Data%20Protection%20in%20India_A%20Critical%20Assessment%20%28663-677%29.pdf



Personal Liberty) and Article 14 (Equality and Equal Protection of laws). But these rights are subject to reasonable restrictions given under Article 19(2) which can be imposed by the State. Judicial Activism has brought right to privacy within Article 21 which talks about Right to Life and Personal Liberty. Article 21 provides that “no person shall be deprived of his life or personal liberty except according to procedures established by law”. On the basis of this provision, the Supreme Court observed that “those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law”.

The Supreme Court in *Kharak Singh v State of UP*¹, observed that the right to privacy is an essential ingredient of life and personal liberty. Similarly *PUCL v Union of India*², the Court observed that privacy is a part of life and personal liberty as enshrined in Article 21 and the said right cannot be curtailed except by the procedure established by law. In *Gobind v State of MP*³, the SC observed that privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. The court however ruled in *Malik Singh v State of P & H*⁴, while exercising surveillance over reputed bad characters, habitual offenders, and potential offenders the police should not encroach upon the privacy of a citizen so as to offend his rights under Article 21 and Article 19(1) (d). The decision given by SC in a revelent case weakens the right to privacy because it allows the public authorities to obtain evidence illegally. In *V.S Kuttan Pillai v Ramakrishnan*⁵, the court held that general warrant for searching and seizing listed documents would not entail invasion of privacy even if the search did not yield any result because of counter availing state interests. In *State of Punjab v. Baldev Singh*⁶, that for a search of a person the safeguards provided Sec. 50 of the Code of Criminal Procedure are mandatorily to be followed. The invasion of a person has been given a protection through insistence on a procedural safeguard but the court has not ruled that evidence obtained in breach of Sec. 50 safeguards would be impermissible evidence. In *R. Rajagopal v State of Tamil Nadu*, the Court held that the petitioners have a right to publish what they allege to be the autobiography of Auto Shankar insofar as it appears from the public records, even without his consent or authorization. But if they go beyond that and publish his life story, they may be invading his right to privacy, and then they will be liable for the consequences in accordance with law. Similarly, the State or its officials cannot prevent or restraint the said publication.

¹ AIR 1963 SC 1295

² (1997) 1 SCC 301

³ (1975) 2 SCC 148

⁴ AIR 1981 SC760\

⁵ AIR 1980 SC 185

⁶ AIR 1999 SC 2378



In *Peoples Union for Civil Liberties (PUCL) v. Union of India*, right to privacy of an electoral candidate was held not violated by publications of details of his criminal antecedents and/or his assets and liabilities. It has been held that a doctor's disclosure of a person's incurable physical ailment (HIV) to the relatives of the one to whom he was to get married was not violative of right to privacy. Doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amount to the invasion of right to privacy which may sometimes lead to the clash of one person's "right to be let alone" with another person's right to be informed.¹

It was held that in divorce proceedings an order to undergo medical examination on strong grounds of necessity to establish a contention was held not invasive of right to privacy. Public policy requirements were permitted to prevail over private interests.²

In *District Registrar and Collector v. Canara Bank*³, the court struck down Sec. 73 of the Indian Stamp Act, 1899 as amended by the Andhra Pradesh Act (17 Of 1986) as permitting an over broad invasion of private premises or the homes of persons in possession of documents in a power of search as seizure without guidelines as to who and when and for what reasons can be empowered to search and seize, and impound the documents. The court however held that no right to privacy could be available for any matter which is part of public records including court records.

Three inferences can be drawn from the above decisions are:

- Right to privacy exists and the unlawful invasion is punishable.
- Constitutional recognition exists for right to privacy
- Right to privacy is not an absolute right

INTERNATIONAL CONCEPTS OF PRIVACY:

Article 12 of Universal Declaration of Human Rights (1948) states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attack upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."

Article 17 of International Covenant on Civil and Political Rights (to which India is a party) states "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondence, nor to unlawful attacks on his honour and reputation"

Article 8 of European Convention on Human Rights states "Everyone has the right to respect for his private and family life, his home and his correspondence; there shall be no interference by a public authority except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being

¹ AIR 1999 SC 495

² AIR 2003 SC 3450

³ (2005)1 SCC 496



of the country, for the protection of health or morals or for the protection of the rights and freedoms of others.”

INTERNATIONAL DATA PROTECTION LAWS:

National laws governing privacy and data protection do exist in some countries¹. For instance Australia has a Privacy Amendment (Private Sector) Act, 2000, Canada has the Personal Information Protection and Electronic Documents Act, 2000, New Zealand has the Privacy Act, 1993, and UK has the Data Protection Act, 1998. But some countries in the world including India have no legislation at all². Some international legal instruments which help in providing the basis for development towards an international harmonisation of principles relating to data protection and right to privacy in the digital era i.e. the 1980 OECD Guidelines³, the 1981 Council of European Convention⁴ and the 1995 European Commission Directive⁵.

Organisation for Economic Cooperation and Development (OECD) Guidelines

The OECD guidelines on the protection of privacy and Trans border and flows of personal data have provided general guidance on the handling of personal information in the public and private sectors since 1980. The OECD Guidelines represents an attempt to balance the conflicting priorities of data protection and the free flow of information. The most fundamental limitation of these guidelines is that they have no legal force. They are not embedded in any convention.⁶

Council of European Convention

Unlike OECD, which is essentially concerned with the economic development of its member states, the Council of Europe has a border political mandate. The convention set forth the data subjects right to privacy, enumerates a series of basic principles for data protection, provides for Trans border data flows, and call for mutual assistance between parties to treaty including the establishment of a consultation committee and the procedure for future amendment to the Convention⁷.

¹ National data protection laws around the globe, pp. 1-5

² OECD report, “Privacy and Data Protection-Issues and Challenges”, Paris, 1994

³ Organisation for Economic Cooperation & Development, “Recommendations of concerning Guidelines Governing the Protection of Privacy and Trans border Flow of Personal Data”, 2391980, C(80) 58(Final).

⁴ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28-1-1981 (Entered into force on 1-10-1995), Council of Europe.

⁵ European Parliament and Council Directive 95/46/EC, 24-10-1995 on the protection of Individuals with regard to the Processing of Personal Data & the Free Movement of Such Data, Official Journal of the European Community, 23-11-1995, No. L281, 31.

⁶ Available at <http://www.oecd.org/sti/ieconomy/37626097.pdf>

⁷ Sarah Ellis & Chales Oppenheim, “Legal Issues For Information Professions”, Part III: Data Protection & the Media- Background of the Data Protection Act, 1984 & the European Commission Directive on Data Protection, Journal of Information Science 19(1993), at p. 85.



European Commission (EC) Directives

The EC Data Protection Directives reaffirms the principles outlined in the Councils Convention. The Directives lays down the condition which must be fulfilled for legally processing personal data.

DATA PROTECTION LAWS IN INDIA:

Constitutional mandates:

There is an inherent and natural conflict between right to privacy on one hand and right to information and right know on the other. A law pertaining to data protection should be primarily reconcile this conflicting interests. Thus, the data of individuals and organisation should be protected in such manner that their privacy rights are not compromised.

Statutory Perspective:

The inherent and natural conflict between right to know and right to privacy is also permeating various statutory laws enacted from time to time.

1. **Right to information in cases of venereal or infectious diseases**-section to 69 to 271 of the IPC, 1860 make an act, which is likely to spread infection, punishable by considering it as an offence. The courts should not interfere with the choice of two consenting adults who are willing to marry each other with full knowledge about the disease. It must be noted that in *Mr X v. Hospital Z (II)*¹ a three judge bench of the Supreme Court held that once the division bench² of the Supreme Court held that the disclosure of HIV positive status was justified as a girl has the right to know.
2. **Right to know about the information under the control of a public authority**- in our present democratic framework, free flow of the information for the citizens suffers from several bottlenecks including the legal framework, lack of infrastructure at the grass route levels and an attitude tendency of maintaining secrecy in the day to day governmental functioning. To remove this unreasonable restrictions the Freedom of Information Act, 2002 has been enacted by the Parliament.

INTEGRAL PART TEST: RELATION BETWEEN RIGHT TO PRIVACY AND RIGHT TO PERSONAL LIBERTY

This section of the paper analyses the implied existence of right to privacy under Part III of the Indian Constitution. The Supreme Court in *Surabh Chandni v UOI*³, noted that the Constitution is organic and ongoing in nature. In *Ashok Tanwar v State of HP*⁴, the Court observed that the Constitution should be flexible in nature to meet the needs and address the issues of changing times. Thus, right to privacy being a metaphysical constitutional right should

¹ (2002) 4 SCC (Jour) 12: Madhavi diwan, the right to privacy in the age of information and communications.

² *Mr X V. Hospital Z* (1998) 8 SCC 296.

³ AIR 2004 SC 361.

⁴ AIR 2005 SC 614



be read into the right to personal liberty, otherwise, it would amount to gross constitutional anachronism. Thirty-eight years back in 1978, when the Freedom of Press wasn't a public right, Justice P.N. Bhagwati in the *Maneka Gandhi v. Union of India*¹ had observed that the freedom of press is an important aspect of the freedom of speech and expression. In the process, he laid down the "Integral Part Test". He opined that "even if a right is not specifically named in an Article, it may still be a fundamental right covered by some clause of that Article, if it is an integral part of a named fundamental right or partakes of the same basic nature and character as that fundamental right"² He further noted that the expression "personal liberty" under Article 21 should not be read in a narrow and restricted sense, and "the attempt of the court should be to expand the reach and ambit of the fundamental rights rather than attenuate their meaning and content by a process of judicial construction"³ This approach was adopted by the Supreme Court in *Unni Krishnan v State of Andhra Pradesh*⁴ when they read the term 'life' to include 'education' as one of its essential element promoting good and dignified life. This went on to take the form of the 86th constitutional amendment⁵ which inserted Article 21-A⁶ in the Constitution and made "right to education" a fundamental right under Part III.

Thus, by applying the "Integral Part Test" we realise that right to privacy is, in consequence, and in its true essence, an integral part of the right to personal liberty. "Privacy" mirrors the integrals of "personal liberty" and thus should fall under one umbrella Article. It carries the similar nature and character as the fundamental rights under Article 21⁷.

Moreover, in 2002, the National Commission to Review the Working of the Constitution⁸ recommended a constitutional amendment in the form of Article 21-B⁹, which shall make "right to privacy" a fundamental right under Part III of the Constitution. Moreover, there was also a proposed Privacy Bill in the legislature during the year 2011. The bill was drafted with the objective of creating a statutory Right to Privacy, but is yet to be adopted by the Parliament. Furthermore, Section 3 clause (xi) of the Juvenile Justice (Care and Protection of Children) Act, 2015, provides the "Principle of right to privacy and confidentiality".

¹ AIR 1978 SC 597

² Ibid

³ Ibid at 22

⁴ AIR 1993 SC 217.

⁵ The Constitution (Eighty-Sixth Amendment) Act, 2002, Acts of Parliament, 2002 (India).

⁶ INDIA CONSTITUTION., art. 21-A. 16 while reading implied rights into Article 21

⁷ BASU, D.D., COMMENTARY ON THE CONSTITUTION OF INDIA (9th ed. LexisNexis 2015): Kalyani Baskar (Mrs) v. M.S. Sampooram, (2007) 2 SCC 258; National Legal Services Authority v. UOI, (2014) 5 SCC 438.

⁸ Hall Borg, R.B, Principles of Liberty and the Right to Privacy in LAW AND PHILOSOPHY 183 (Springer Publications 2015).

⁹ Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295



CYBER SECURITY:

Cyber security is applied to computers and networks. The field covers all the processes and mechanism by which computer-based equipment, information and services are protected from unauthorised access, change or destruction. Computer security also includes protection from unplanned events and natural disasters¹. Indian Computer Emergency Response Team² (CERT-In) - this is the national nodal agency for responding to computer security incidence as an when they occur. Through Information Technology (amendment) Act 2008 CERT-In has been designed to serve as the national nodal agency for responding to perform some function in area of cyber security.

Cyber security in India is not up to the mark and is an ignored world. Till now we have no cyber security laws in India. Of course, one or two vague provisions have been incorporated in the information technology Act, 2000 and amendment Act, 2008 of India that happens to be the sole cyber law of India. Even the cyber law of India is weak and ineffective in tackling the fast growing cybercrimes in India. There must be strong and robust law shall be enacted that is also constitutionally and legally sound.

INTERNATIONAL SAFE HARBOUR PRINCIPLES:

There was a need to diminish the divide between the US and the European Community who adopted different approaches to privacy protection to their citizens. The agreement between the EU and the US rests on seven safe harbour principles: notice, choice, onward transfer, security, data integrity, access and enforcement. India could incorporate these principles while formulating legislation in this behalf.

CONCLUSION:

Privacy and data protection are two requirements for the effective functioning of the cyber space. Undoubtedly, the concept of data privacy and protection is at a nascent stage in India. Considering that the international community regards the right to privacy and data protection as a basic human right, India may be under a moral as well as legal obligation to enact privacy and data protection regulations. As mentioned above, India is still struggling for enduring an effective and concrete legislation for data protection. A new legislation dealing specifically with the protection of data and information present on the web is the dire need of the day. However, while drafting the laws, the legislature has to be cautious of maintaining a balance between the interests of the common public and tightening its grip on the increasing rate of cyber crimes.

¹ Available at https://en.wikipedia.org/wiki/Computer_security

² Section 70-B of the Information Act, 2000.