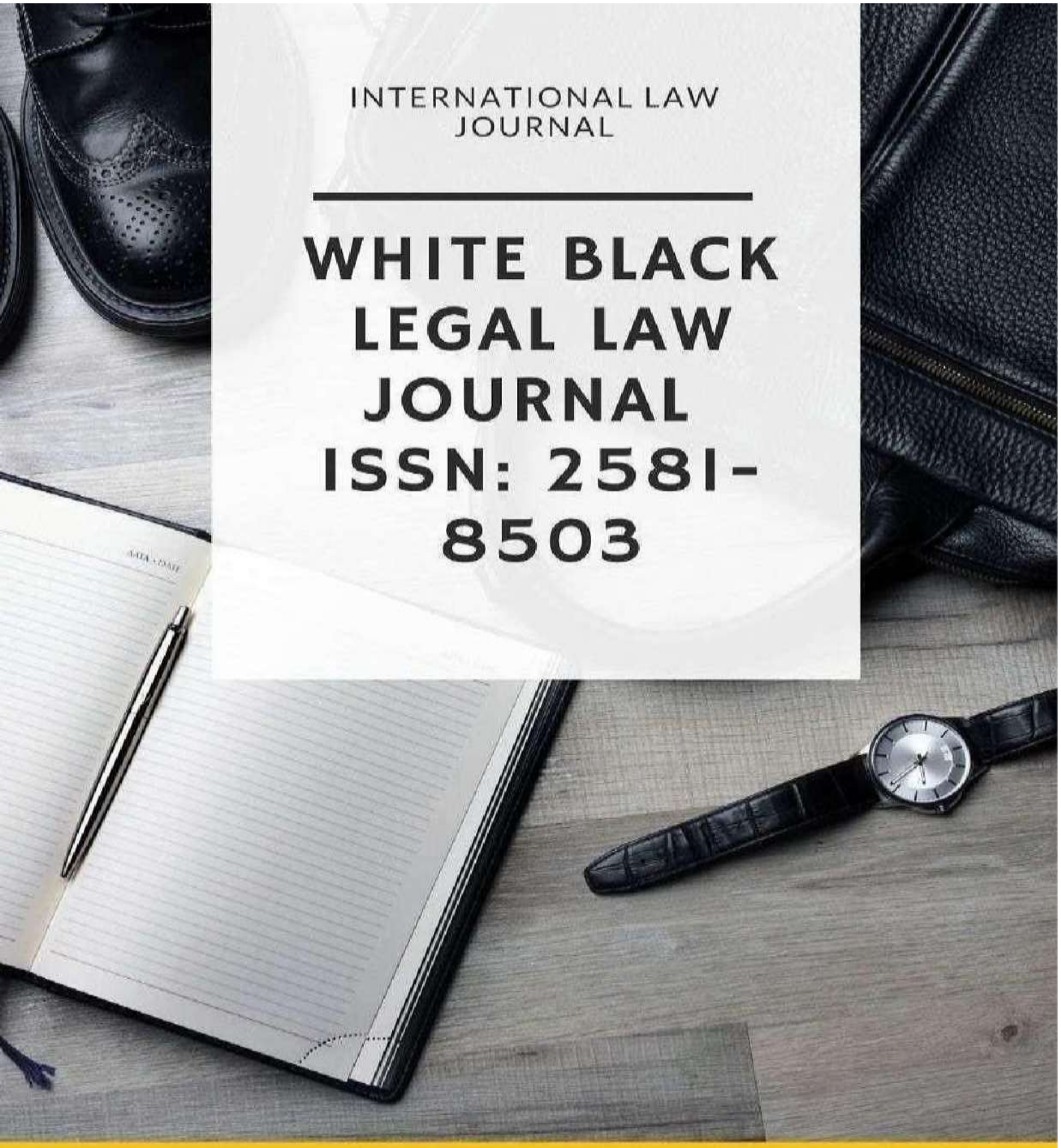

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 6 | April 2026 ISSN: 2581-8503

"LAW IN CYBER SPACE"

AUTHORED BY - PRAGYA TRIPATHI & RAHUL SINGH

ABSTRACT

Every technology has its pros and cons and so has the internet. Cybercrime is the most trending cons and result of the same technology called Internet. It is an illegal act done through the tool of computer. Cybercrime is not a traditional crime but refers to an emergence where a smart traditional criminal step into the new era of technology with the means of computer and internet by using it as a weapon. It is fast- growing and highly increasing crime which easily attracts mainly youth and sometimes start as a fun but the end can be very dangerous. It take place in virtual world called "Cyber Space" which is a mere extension to the real world. It is more trending area of crime and despite of all penal laws, we are lacking to reduce it because of its non-existence of physicality and problem of lack of territory. However to curb this problem we need to guide our own actions as the perpetrator and the victim both are the stakeholders of this virtual world. Though we have all penal laws against cybercrime but still it is spreading its roots in our society and cyber attacks rapidly increasing day by day. And the irony is target of cyber attacks can be anyone and most of the times the government itself. It was in the recent news that Pakistani hackers called "Kashmiri Cheetahs" hacked Thiruvanthapuram Airport and AIIMS Raipur's website[1] which was very disappointing on the part of government that it is lacking in cyber security. So we not only need to protect the lay-man of the society but to protect our government from this cyber threat. As quoted by our Prime Minister Narendra Modi, "Cyber-related risks are a global threat of bloodless war. India can work towards giving world a shield from the threat of cyber warfare".[2] Through this paper I would like to throw light on the cybercrime from the perspective of Indian Penal Laws.

KEYWORDS: Technology, Internet, Cybercrime, Cyber attacks, Penal laws

[1] Express Web Desk, "Thiruvanthapuram airport's website, which was hacked, restored now", The Indian Express, Dec. 28, 1026.
[2] PTI, "World facing 'Bloodless' cyber war threat: Modi", The Hindu, July, 01, 2015.

INTRODUCTION

In the era of modernisation where on one hand we are moving forward with the advancement of technology on the other there are some cons of this modernisation which tries to curb the societal and economic growth of the country. The archaic penal laws since 1860 which deals with the traditional crime like murder, sexual offences, theft, defamation are now inept in dealing as we stepped into the more technological phase. The era of computers brought new social platform for communication, trade and business making our life easy but often this unregulated access to internet invites the misuse of computers as a tool of various illegal acts. There have been various kinds of computer and internet related crimes with the increased growth of internet itself which includes identity theft, unauthorised access to someone else computer most popularly known as 'Hacking', forgery, cyber theft, Trojan, defamation, obscenity and child-pornography. The era of digitisation threaten to leave the traditional laws as these legislation were unable to deal with the modern cybercrime. The problem does not lie in the fact that so many diverse kinds of crimes can be committed using the internet but the fact that existing criminal law might be ill equipped to deal with this 'upgradation' in the methods and media of committing crimes. The challenge which is post can be categorised into two aspects: firstly, the relative newness of the internet and the corresponding antiquity of the present laws in force. Secondly, the irrelevance of geography which poses serious questions with regard to jurisdictional matters that are fundamental for any criminal proceeding to take place[3]

Crime is something which effects ones social reputation as well as economic status. A crime is an act or omission in respect of which legal punishment is inflicted on the person who is in default either by acting or omitting to act and criminal law relates to crimes and their punishment.[4] People generally relate crime with traditional crimes which are defined under Indian Penal Code, 1860 but this so-called technological era gave many more new crime which relate to the computer and internet specific crimes. These crimes are called 'cyber-crime' where computer is used as a tool or weapon to commit crime against any person or property. There is no settled definition of Cybercrime in the traditional Indian Penal Code of 1860 and neither in Information Technology Act, 2000 nor in the Information Technology Amendment Act, 2008.

[3] Nandan Kamath, *Law Relating to Computers Internet & E-commerce*, pg210 (Universal Law Publishing Co., New Delhi, 5th edn., 2012).
[4] K.I. Vibhute, *PSA Pillai's Criminal Law*, pg 4, (Lexis Nexis, Gurgaon,11th edn 2013)

In this paper we will examine whether the existing laws in India are adequate to deal with cybercrimes and whether there is a need for a uniform standard international regime to regulate the internet.

As discussed earlier a crime constituted must be accompanied by a wrongful act i.e. actus reas combined with the wrongful intention i.e. mens rea. The maxim *actus non facit reum nisi mens sit rea* means an act does not make one guilty unless the mind is also legally blameworthy. The actus rea in cybercrimes is easy to identify but is not always easy to prove. Mens rea refers to the state of mind of the person committing the crime and comprises of various mental attitudes including intention, recklessness and negligence.

INFORMATION TECHNOLOGY ACT, 2000

Emergence of technology and its misuse go hand in hand, and increased to its maximum level in such a way, that it was impossible to tackle this issue. Then there also arises a need of strict statutory laws, to regulate the criminal activities in the cyber space and to protect the technological advancement system[5]. Before 1970 there were no computer specific laws which deals with the problem of cybercrime. In the year 1970, the first legislation was made by the German State of Hesse which was computer specific, called the 'Data Protection Act, 1970'. After 30 years the Indian Parliament passed a sui generis statute known as "**INFORMATION TECHNOLOGY ACT, 2000**" and finally the Indian cyber legislation came into force on 17th October, 2000.

Objectives of the Information Technology Act, 2000[6]

The primary objective of the aforesaid act was "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."

[5] Prof. (Dr.) KPS Mahalwar, Praveen Kumar, Varun Kumar, "Cyber Crimes and the law: Evaluation of the Information Technology Act,2000," (2011) PL September S-2
[6] Information Technology Act,2000

The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cybercrimes.

INFORMATION TECHNOLOGY AMENDMENT ACT 2008:

Information Technology Act is an act of modernisation which has to move with time over time. As the new technology is being created every day in the society, which is also increasing in cybercrime. So it was unable to meet the demands of time and due to several debates, doubts and criticism the Information Technology Act was amended in 2008 as and made effective from 27th October 2009. Indian legislature came up with the sui generis protection laws to strengthen the grip in cybercrimes and to define the cybercrimes and its penalties and punishment in a stringent and definitive manner.

Some important features of Information Technology Amendment Act 2008 are:

- Putting more emphasis on data privacy.
- Added electronic signature
- Maintaining the register in cyber café made mandatory
- Make changes in role of intermediaries
- Inclusion of some additional cybercrimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

JURISDICTION ISSUES IN CYBER SPACE

Under Section 1(2) of the Information Technology Act, the enforcement of this act shall extend to the whole of India and also applies to any offence or contravention there under committed outside India by any person. The Act is applicable to whole of India except the state of Jammu and Kashmir. The provisions of Indian Penal code are applicable to Information of Technology Act as per the provisions of Section 77 of Information Technology Act provides that the compensation, penalties and confiscation under the IT Act does not release the offender from liability under any other law. Any crime committed by Indians living in foreign soil will also be held liable.[7] Section 4 of Indian Penal Code provides for application of penal code to extra

[7] Indian Penal Code, 1860 (Act 45 of 1860), s. 3

territorial offences. It is crystal clear that for traditional crime committed by an Indian either in India or in any foreign country can be tried but cybercrime knows no boundaries. Accused can operate from any country while committing the crime, the problem lies in extraditing the offender back to India. Unless they are found in the territory of our country, our penal laws cannot be made to them.[8]

There are diverging views whether these cybercrimes can be restricted to jurisdiction of a nation or not. There are two divergent school of thought one being Cyber libertarianism who believe that cyber space cannot be regulated and the school of thought being Cyber paternalism who believe that the cyber space can be regulated. Cyber libertarianism contend that regulations founded upon traditional state sovereignty, based as it is upon notions of physical borders cannot functions effectively in cyber space as individual move seamlessly between zones by differing regulatory regimes in accordance with their personal preferences.[9] One of the classical example can be given as which ingredients constitute obscenity in India would not be the same for other sovereign nations. The differences in the categorisation is a result spectrum of community standards which ranges from an extremely conservative to an extremely liberal one.

Cyber paternalism do not believe that cyber space is immune from regulatory invention by the real world regulators. The technological developers presumes the roles of traditional political governance and regulate the network by its very architecture.[10]

Traditional requirements generally requires two criteria, firstly the place where the defendant resides or secondly where the cause of action arises, however both of these criteria's are difficult to establish in context of internet. The main problem emerged while addressing the issue of jurisdiction was that there is no statehood in cyber space. The Budapest Treaty 2001 is the first ever international convention on cybercrime. It is the first treaty on criminal offence against, with or with the help of computer network or internet.

In order to complement the understanding of the cyber offences under the Act, it is important

[8] D. Latha, "Jurisdiction Issues in Cyber Crimes" (2008) 4 LW (JS) 84
[9] Andrew Murrey ,*Information Technology Law: The Law and* Society, pg48 (Oxford Publication, New Delhi, 2010)
[10]Andrew Murrey ,*Information Technology Law: The Law and* Society, pg61 (Oxford Publication, New Delhi, 2010)

that the criminal law of India, which has been codified in the Indian Penal Code, 1860, and the code of criminal procedure, 1973 should also be taken into consideration. The penal code deals specifically with the offences whereas the Criminal Procedure Code is all about criminal procedures. While the penal code is substantive law, the Criminal Procedure Code is the adjective law. The object of the Code of Criminal Procedure, 1973 is to provide machinery for the punishment of offences against the substantive criminal law, for example the Indian Penal Code, 1860. The Code of Criminal Procedure, 1973 also provides machinery for punishment of offences under other acts.

Hacking

In real world when anyone encroaches someone's property without any authorisation or without the consent of the owner then it constitutes the offence under Tort law. But what about situation where someone without the authority access the banking or social networking account or the website of anyone. In technological sense it is called Hacking. Generally when people hear the word hacking they relate it with the cyber-terrorism. Hackers are the people who have good computer knowledge and they know all the technicalities of the cyber world and they use these skills to attack the computer system of others, release viruses and break the password. Hacking is an illegal access which comprises entering of the secured and stored data of someone's computer, and vitiate, modify, change or stole the data.

Instead of having sui generis protection mechanism, we are at the failure to control or even reduce this problem. This is so serious and uncontrollable problem that even the technological companies in the world are not able to cope up with their perpetual attacks.[11] Generally hacking starts with the fun and ends with the damaging the computer of someone and misuse their personal data which is punishable. Initially, the intention behind the hacking was not malafide but elvish.

Section 66 of IT Act deals with hacking as "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"[12]. Whereas there is no specific definition

[11] Abhishek Jaisawal, "Cyber Hacking Laws" available at http://www.legalservicesindia.com/articles/cyhac.htm
[12] Information Technology Act, 2000 (Act 21 of 2000), s. 66

given under the Indian Penal Laws however, when it comes to hacking, section 441 criminal trespass read with the IT Act provisions. In this sense, website, computer system or stored data is the property of someone and whoever enters into or upon the property, without the authority, constitute the offence.

There are several examples where websites of various governmental departments have been hacked. It can easily say that even government is failed to protect its own official websites. It was in the recent news that Pakistani hackers called "Kashmiri Cheetahs" hacked Thiruvanthapuram Airport and AIIMS Raipur's website which was very disappointing on the part of government that it is lacking in cyber security. So we not only need to protect the lay-man of the society but to protect our government from this cyber threat.

"Awareness isn't about acting unethically in our day-to-day activities by defacing Web sites, promoting unfair discriminatory policies or generally being over reactive and hysterical. Awareness is about applying the necessary access controls and requiring authentication and appropriate authorization to access of information"[13]

Hackers infringe the penal laws and starts from hacking the school website to hacking the government official website. There can be several reasons why hackers indulge in illegal act. For example, sometimes hackers access the website of others just to show off or just to win the challenge. So to not getting into this problem one has to be more attentive and vigilant. Netizens should always remember to log out their account whenever they access it.

CYBER OBSCENITY

The issue of obscenity has always been a complex one as it involves other related issues like decency and morality. There is no straitjacket principles to judge obscenity. It is almost next to impossible to reduce obscenity in the virtual world. There is no doubt that computer and internet has changed the lives of people and bring immense transformation in their lives. It has also made easy for the people to communicate through messaging, video calling and social networking sites like Facebook, Twitter etc. Many netizens upload their personal pictures and video in these social networking sites without even realising that this could be the worst

[13] Wilson M. (2003, April 09). War, ethics and security. Computerworld. Retrieved July23, 2004 from http://www. computerworld. com/printthis/ 2003/0, 4814,80185,00.html

nightmare of their lives.

It is not easy to give the exact definition of obscenity and pornography as the ingredients of both the concepts are different in nation to nation. For example, some features which constitute obscenity in Indian culture could be normal in the American culture because of ideological and cultural differences.

Obscenity is not defined in Indian Penal Code but ingredients of traditional obscenity and pornography are defined under section 292-294 of Penal Code of India whereas cyber obscenity and pornography are defined under section 67 of Information Technology Act, 2000. Section 67 of the IT Act makes the obscenity in electronic form punishable.

In a landmark judgment, decided by Bombay High Court in ***RanjitUdeshi and Ors. Vs. The State,***[14]a test has been laid down to identify what material, work or content shall amount to being obscene by interpreting the word *"obscene"* as that, which is *"offensive to modesty or decency, lewd, filthy and repulsive."*

IT Act, 2000 came up with cyber or online obscenity because IPC did not include obscenity in electronic form. By virtue of this act the ingredients of obscenity in electronic form are[15]-

- acts which publishes transmits, causes to be published
- "any material", video files, audio files, text files, images, animations and even CDs, Web sites, Computer, Cell Phones etc.
- which is lascivious, appeals to prurient interest, and tends to deprave or corrupt of minds of the person.

After the amendment of IT Act, several changes made in the Amendment Act regarding the provision of obscenity[16]-

- Violation of privacy (coupled with cyber obscenity)
- Publishing or Transmitting obscene material in electronic form

[14] AIR 1962 Bom 268.
[15] Information Technology Act, 2000 (Act 21 of 2000), s. 67
[16] Dr. Shashikant Hajare, Mr. Ashok Wajde, "Obscenity in cyberspace: response of Indian cyber laws" ISSN:2349-7858 :SJIF 2.246:Volume 2 Issue 2.

- Publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Section 67 A)
- Child pornography (Section 67 B).

Punishment: Any person who is tried under this section, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.[17]

CYBER STALKING

Generally stalking is associated with the act of a person's repeated harassing and threatening behavior towards another person. Cyber Stalking simply refers to the use of electronic medium to repeatedly harass and threaten the victim repeatedly over a period of time. Cyber Stalking is no more than the reflection of the stalking in the real world as in both the instances it generally involves former intimates however it also involves stranger stalking. Stalkers are generally motivated by their desire to control the victim as what me started as light spoofing of the other persons online social profile may turn into sending threatening messages, absurd and disturbing calls in the middle of the night. The general perception of the fact that cyber stalking is not as serious as it is void of any physical contact is highly inaccurate as the victim faces more threat as compared to the stalking because the non- confrontational, impersonal and anonymous nature of internet communications actually encourage the offenders. Cyber stalking is more specific as compared to spam's as they specifically target the victim to manifest the stalker's obsession. The Penal Code of 1860 by the recent criminal amendment of 2013 inserted the provision of stalking as a gender specific offence wherein the victim would only constitute a woman. The Section 354D of IPC defined stalking as *: "(1) Any man who-*

- *follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet,*
- *email or any other form of electronic communication, commits the offence of stalking;"*

The punishment for a first time offender is may extend to a term of 3 years imprisonment which shall be accompanied by fine and for repeated offenders the term of imprisonment may extend

[17] Information Technology Act, 2000 (Act 21 of 2000), s. 67

to 5 years and shall be accompanied with fine.

Prior to the Amendment of 2008 the Information Technology Act of 2008 was inept to deal with the cybercrime of stalking. Section 66A of the Act penalizes any person who sends any grossly offensive information or any information which the stalker knows to be false but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred through electronic mail or any computer resource or communication device shall be penalized with a term which may extend up to 3 years and fine.

However Section 66A was repealed in the landmark case Shreya Singhal v. Union of India[18] wherein a division bench of Supreme Court said that such a law hit at the root of liberty and freedom of expression, the two cardinal pillars of democracy. The Supreme Court said section 66A first and foremost infringes the fundamental right to free speech and expression and is not saved by any of the eight subjects covered in Article 19(2) as the causing of annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will are all outside the purview of Article 19(2) was vaguely worded and allowed its misuse by police.

The provision of Information Technology Act was more broader as compared to the Penal Code of 1860 as it defined Cyber Stalking in a gender neutral perspective. The repealed provision provided an opportunity to genuine victims of cyber harassment to obtain immediate relief against content that may be insulting or injurious in nature whose repeal has now made Police authorities toothless in dealing with the growing menace of cyber bullying. A multi-racial, multi-cultural country like India, where free speech is susceptible to misuse on sensitive grounds of communal, political and religious bias, is not prepared for such an absolute and unrestrained right. What we need is to be able to exercise the right to speech freely but on practical and workable grounds i.e. within specific boundaries.[19]

The victim of cyber stalking can now avail the criminal remedy under the Penal Code as discussed above or the Civil remedy of injunction wherein the either damage or apprehended damages which involve imminent danger of substantial kind or an irreplaceable injury. The

[18] AIR 2015 SC 1523
[19] Partha Pati, Sanjana Sinhraoy (2015, April 24) "Section 66a: its repeal and its after effects" available at (http://www.legallyindia.com/views/entry/section-66a-its-repeal-and-its-after-effects

victim can also avail damages for emotional and physiological harms under the civil remedy. However, the present law is inadequate in terms of the demands of gendered equality. The Indian Criminal System needs to become more sensitive to tackle the societal demands and bring forth a more comprehensive and gender neutral laws.

Conclusion

The Information Technology Act, 2000 is an infant piece of legislation which was formed to set definite rules which would govern the business transactions over the net. The emergence of economies of developing nations facilitated breeding ground for new forms and manifestations of cybercrimes. Hence, to curb the increasing menace the Parliament brought forth an Amendment in 2008 with the prime focus on tackling these cybercrimes with more stringent and penal reforms. The biggest challenge faced by the policy makers is to keep pace with the Technology and concurrently making policies which not only regulate the technology but also facilitate it's growth. The Amendment has faced various criticism as the penalty has been reduced from five years to three years in various offences like obscenity. Along with this many offences which were non bailable previously have been made bailable offence which would provide ample opportunity to the cyber criminal to immediately go and evaporate , destroy or delete all electronic traces and trails of his having committed any cybercrime, thus making the job of the law enforcement agencies to have cybercrime convictions, a near impossibility.[20]

The conviction rate of cyber offences is still minimum. The law enforcement agencies are more comfortable with trying the case on traditional offences like fraud, robbery, defamation, criminal trespass rather than relying on the sui generis mechanism provided under the Information Technology Act. There is a dire need of sensitization programs for Judges and police officials. There should be a harmonious consent among all the nations to form a broad umbrella protection of a uniform legislation to govern the cybercrimes.

[20] Maneela, "Cyber Crimes: The Indian Legal Scenario", 11 US China L. Rev. 570 2014